INTERNET SECURITY ALLIANCE

ecoDa
The European Voice of Directors

CYBER SECURITY RISK HANDBOOK

KEY TOOLKITS

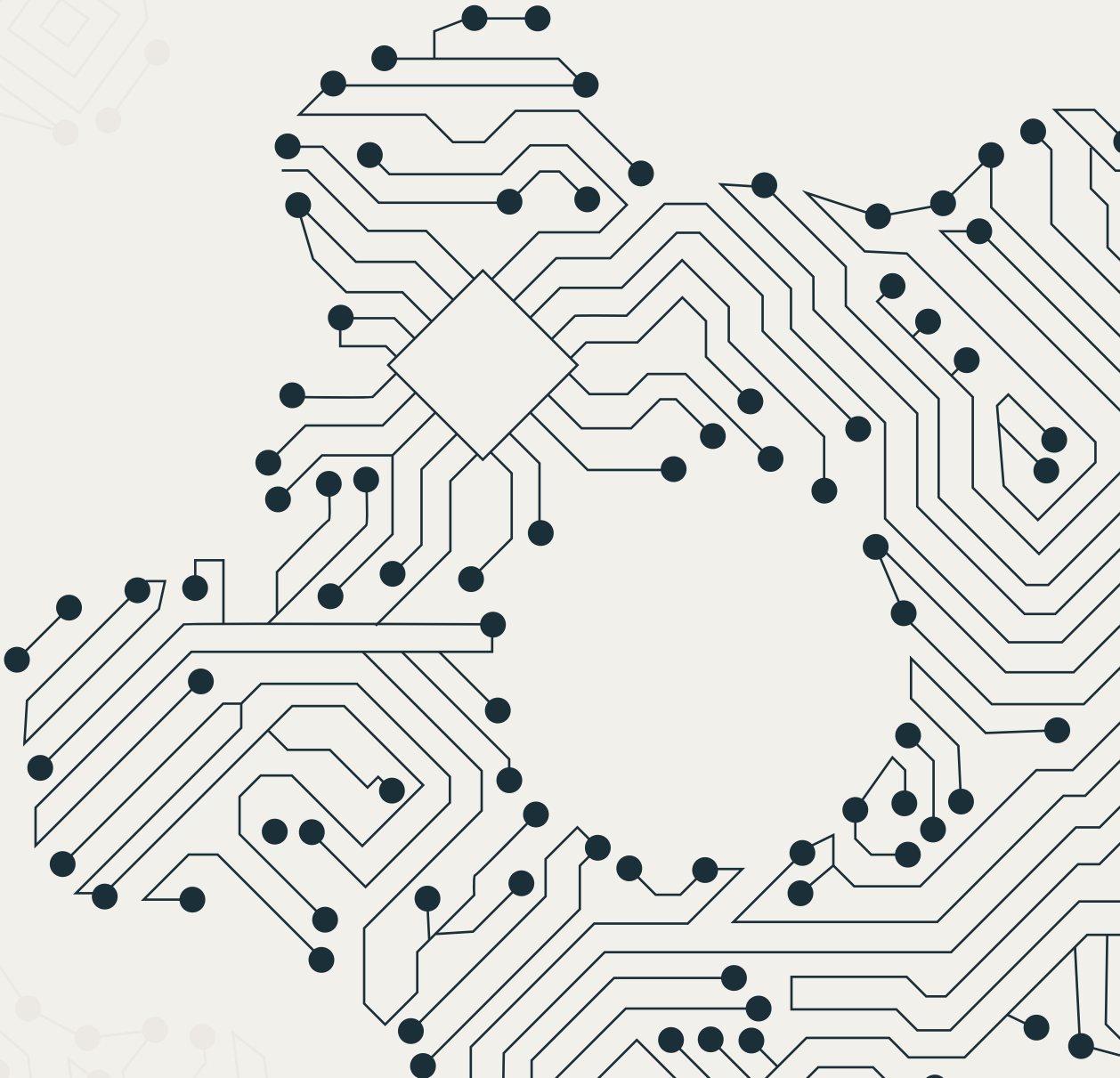


TABLE OF CONTENTS

Tool A

RANSOMWARE READINESS

- WHAT IS RANSOMWARE AND WHY IS IT UNIQUE FROM OTHER CYBER THREATS?
- THE EU CASE
- QUESTIONS BOARDS SHOULD ASK SENIOR MANAGEMENT ON RANSOMWARE

TOOL A

WHAT IS RANSOMWARE AND WHY IS IT UNIQUE FROM OTHER CYBER THREATS?

Ransomware is a tool for extortion. It is a type of malicious software (malware) used by threat actors to block access to data or systems. Ransomware encrypts its target until the victim pays a ransom, usually with specific deadlines and requirements to be paid in cryptocurrency.

In 2022, it took on average almost one month for an organization to recover from a ransomware attack[1].This means one month of lost opportunity, extra device costs, the ransom itself, and more. Plus, companies that became a target of an attack once, are more prone to subsequent attacks since they get earmarked as having low-grade cyber-security measures. In 2022, the average cost of reparations for an organization in the United States was approximately $2.0 million dollars. In 2023, the average cost to recover from a ransomware attack was approximately $2.73 million dollars, an increase of almost $1 million dollars from 2022[2]. With more than 150 active variants as of 2022, ransomware has become both cost-effective and a service-based attack for cyber criminals. According to Top10VPN's Hacking Tools Price Index, malware can be purchased for as little as $45, while tutorials on how to construct attacks are available for only $5[3]. Ransomware-as-a-Service (RAAS) can even be purchased on a monthly subscription basis[4]. As mentioned in the Principles section of this Handbook, the economics of cybersecurity tend to be upside down, as the cost to commit an attack is far less expensive than the cost of securing against, mitigating, and insuring organizations. Cybersecurity insurance is costly; accordingly, boards should ensure their management teams have clear contingencies, situational awareness, and readiness to respond to an attack. With the recent rise of dual ransomware attacks, the stakes for companies are higher than ever before.

THE EU CASE[5]

In March 2023, one of Barcelona's top public medical centres, Hospital Clinic, suffered a ransomware cyber-attack. According to EU Cyber strategy, the Cybersecurity Agency of Catalonia began to take action minutes after the criminal contacted the hospital. RansomHouse, who acknowledged the attack, published sensitive medical and financial data of patients and employees, after the hospital and authorities denied paying a $4.5 million ransom. In total, hackers stole 4.4 terabytes of data. The police launched a 'cyberpatrol' on the internet and also on the 'deep web' to locate the data and remove all the information from the system 'as quickly as possible'. Even so, the consequences of the cyberattack lasted months and collaterally affected banks and even the payment system of an airline company. The Catalan data protection authority (APDCAT) investigated into Hospital Clinic's data protection tools, as it could be a sanctioning motive after data was hacked and published.

1 Veeam, "2023 Global Report: Ransomware Trends", 2023, https://www.veeam.com/analyst-reports/trends-report-ransomware_wpp.pdf

2 Sophos, "State of Ransomware 2024", 2024, https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf

3 Simon Mongliano, "Darknet Market Price Index: Hacking Tools", 2018 https://www.top10vpn.com/privacy-central/cybersecurity/dark-web-market-price-index-hacking-tools-us-edition/

4 Kurt Baker, "Ransomeware as a Service (RAAS) Explained: How It Works and Examples," 2023

5 Clinic Barcelona, "Computer attack on the FRCB-IDIBAPS" , 2023 https://www.clinicbarcelona.org/en/news/computer-attack-on-the-frcb-idibaps

TOOL A

QUESTIONS BOARDS SHOULD ASK SENIOR MANAGEMENT ON RANSOMWARE

Readiness

1. Is there a playbook for ransomware that includes responsibilities, processes, and expected outcomes? What role, if any, do you need the board and c-suite executives to play in light of an attack?

2. What are our cyber capabilities and/or countermeasures to deal with ransomware attacks? Boards should look for answers that may include the following:

   a. Use a backup system and routinely check it for data integrity and confirm it is operational;

   b. Participate in cybersecurity information sharing.

3. What percentage of coverage do these capabilities provide across our digital/IT estate?

4. Does our cyber insurance policy cover ransomware specifically? Here are some specific items to consider asking about:

   a. Premiums for ransomware policies have increased in recent years. Would it be more cost effective to self-insure? What advantages do formal insurance policies present to our organization's cybersecurity infrastructure?

   b. Some business policies such as extortion policies may cover losses related to ransomware. Does our policy have that coverage?

5. Are employees trained on how to identify and report if they suspect a ransomware event is occurring? Here are some follow-up questions boards can ask to gauge the depth of the program:

   c. Is our organization providing guidance on handling infected and noninfected computers?

   d. Have our front-line managers worked with IT and information security to communicate alternative methods for business-critical functions (e.g., email, payroll, production).

Backup and Recovery

1. How are our system backups maintained, tested, and measured for resiliency? One follow-up question to consider asking:

   * Does the implementation of backups include reporting, metrics, and ongoing monitoring requirements?

2. In the event of a ransomware attack, are we confident that our IT systems can be restored within our specified recovery plan objectives? Are we including third-party systems and capabilities (e.g., cloud-based software)?

   * When was the last real-time inspection of our cybersecurity posture? How can we be sure that the backup data to re-establish operations is not also infected with ransomware?

3. Do our system backup and recovery partners' response times align with our current timelines in our recovery plan?

Suppliers and Partners

1. Do we monitor critical third parties for ransomware attacks (those we share data with and/or have network connectivity to)? When receiving answers about this question, boards can look for details about the following:

   a. Training supply-chain personnel to recognize cybersecurity risk and enabling mitigation activities

   b. Third-party due diligence throughout the proposal, selection, and onboarding processes

   c. Vendor-risk management framework in place with appropriate stakeholders involved and with a direct owner of this function.

2. Do we require specific ransomware and/or incident reporting from third parties within our contracts and agreements? Directors can consider asking for a follow-up:

   * Is cybersecurity expertise leveraged during the negotiating and contracting process?

3. As part of our enterprise vendor risk management program, do we assess (and reassess) any third parties to understand their cyber risk posture?

Response Exercises

In general, it's important to note that the specific response may vary depending on the nature and severity of the cyberattack, the industry of the affected company, and the applicable laws of the EU member state where the incident occurs. Companies should seek guidance from legal counsel or cybersecurity experts to ensure they are following the appropriate procedures and fulfilling their legal obligations.

In all cases, play-roles and rehearsals of cyber-attacks are important to be trained to react under pressure.

1. Is there a clearly communicated line of accountability in the event of an attack? Are there plans for ransomware tabletops/simulation exercises so that our organization can form muscle memory around employee roles in such an event?

2. Are there clear thresholds related to the materiality of an attack, including triggers for engagement of senior management and/or the board?

3. Are we ready to coordinate with law enforcement in the event of a ransomware attack?

   a. In cases of severe cyberattacks or suspected criminal activity, companies should involve local law enforcement agencies. They will coordinate with other agencies if necessary. The European Cybercrime Centre (EC3 or EC)[3] is the body of the Police Office (Europol) of the European Union (EU), headquartered in The Hague, that coordinates cross-border law enforcement activities against computer crime and acts as a centre of technical expertise on the matter.

   b. In the case of a cyberattack on a company within the European Union, each EU member State has its own designated cybersecurity authority or point of contact for reporting cyberattacks. Companies can report cyberattacks to ENISA through their Incident Reporting System (IRS). This platform allows for secure and confidential reporting of incidents, and ENISA can provide assistance and guidance to affected organizations. https://www.enisa.europa.eu/topics/incident-reporting.

4. **Additional Considerations:** If a cyberattack involves the compromise of personal data, companies must also comply with the GDPR's breach notification requirements. This includes notifying affected individuals and the relevant data protection authority within prescribed timeframes. Companies may also need to report cyberattacks to their insurance providers, depending on the terms of their cyber insurance policies.

5. Does management have a clear stance on paying or not paying a ransomware demand? If an incident causes management to recommend paying a demand, have we done a walkthrough with decision-makers on how the process would work?

    * Does the organization have appropriate access to a cryptocurrency wallet and cryptocurrency expertise to make a payment?

Communications

1. Is there a concise communications plan across cybersecurity, technology teams, and senior management? Here are some items for boards to consider asking follow-up questions about:

    a. When and how company officers and employees will be notified of the disruption?

    b. When and how business partners and key external parties will be notified?

    c. Who will be responsible for preparing and delivering a public statement on the disruption?

    d. What the timeline is for acting on regulatory, disclosure, or compliance requirements, and who will be involved?

2. Does the plan include holding statements for various audiences (e.g., employees, customers, regulators, media)? Here are some items to consider:

    * Keep company officers, employees, business partners, and the public informed as incident investigation progresses.

Tool B

ASSESSING THE BOARD'S CYBER RISK OVERSIGHT EFFECTIVENESS

- OBJECTIVE OF THE TOOL

- UNIDENTIFIED RISK DURING ACQUISITION DUE-DILIGENCE LED MARRIOTT DIRECTORS TO FACE VIOLATION OF SECURITY LAW CLAIMS AND PERSONAL LIABILITY LAWSUITS

TOOL B

OBJECTIVE OF THE TOOL

This tool helps directors identify which questions to ask to assess their own understanding of the organization's cybersecurity, to ask senior management to assess their effectiveness, and outlines a numerical scale for assessing the board's cyber risk oversight effectiveness. The aim of this tool is to establish a cyber governance process led by the board.

Board leaders wishing to incorporate a cybersecurity component into their board's recurring self-evaluation can use the questions in the table below as a starting point.

Questions Directors Can Ask to Assess their Board's Cybersecurity Understanding

1. Who on our board possesses qualifiable cybersecurity expertise? What is that expertise?

2. Can all directors effectively contribute to a robust conversation with management about the current state of the company's cybersecurity? In which areas does our lack of knowledge/understanding of cyber matters prevent effective oversight?

3. Are we able to effectively interpret/assess management's presentations and their answers to our questions?

4. Do we thoroughly understand the most significant cyber threats to this business and what impacts they could have on the company's strategy and ultimately on its long-term growth?Do we receive and understand the implications of a gap-analysis as part of the cybersecurity management reporting? Can the board assess the adequacy of necessary cybersecurity measures?

5. Do we understand security-related legislation and regulation changes that could affect the company? What is the potential impact?

6. Do we know if an Incident Response Plan and playbook(s) exist and what our role is, if any?Is there awareness around if the company have insurance that covers cyber events, and what exactly is covered? Is there director and officer exposure if we don't carry adequate insurance? What are the benefits beyond risk transfer of carrying cyber risk insurance?

7. Do we understand how materiality of an incident is determined, and by whom within our organization? Do we have processes in place for making the proper disclosures when a risk comes to fruition?

USE THE NUMERICAL SCALE TO INDICATE WHERE THE BOARD'S CULTURE GENERALLY FALLS ON THE SPECTRUM SHOWN BELOW							ACTION ITEM
Statements Indicating Lagging Practices	*Range Indicator (Circle Number Closest to Practice Maturity)*					*Statement indicating leading practices*	
We classify cyber risk as an IT or technology risk.	1	2	3	4	5	We classify cyber risks as enterprise-wide strategic risks.	
Our cybersecurity discussions with management focus primarily on reviews of past events (e.g., historical breach data).	1	2	3	4	5	The board reviews regular industry-related threat updates and participates in regular complex breach exercises, or tabletop scenarios applicable to real-world risks.	
The board receives information about cybersecurity exclusively from management.	1	2	3	4	5	In addition to management reporting, the board receives firsthand information about cybersecurity from non-management sources.	
Information about emerging cyber threats or potential issues is filtered through the CEO.	1	2	3	4	5	The CEO encourages open access and communications between and among the board, external sources, and management about emerging cyber threats.	
Board relies on expertise of one or two functional leaders/experts in cybersecurity to evaluate management's plans and assumptions on cybersecurity risk and strategy.	1	2	3	4	5	The board is broadly educated on cybersecurity concepts and best practices that allows for all directors to engage in a discussion on cybersecurity with other board members and management.	

CASE IN POINT

Unidentified Risk During Acquisition Due-Diligence Led Marriott Directors to Face Violation of Security Law Claims and Personal Liability Lawsuits

In August 2018 Marriott International acquired Starwood Hotels and Resorts Worldwide for$13B to expand the hotel chain to the world's largest, merging loyalty programs as a differentiator for corporate travel departments. However, the Marriott's board failed to identify a data breach in the Starwood guest reservation database from 2014 resulting in the loss of sensitive data for more than 380 million people. Sensitive data included: names, payment card data, passport information, travel companions, and home addresses. Even though the breach occurred two years prior to the acquisition, Marriott learned about the breach in September 2018, one month post-acquisition.

All 50 states and District Court Attorney Generals, the SEC, FTC, and U.S. Senate and Congress committees, along with others opened investigations were launched. Marriott Directors were personally named in U.S. Court filings, defending their oversight in court. It was determined that the Marriott board acted in good faith to fulfil their oversight duties. However, the litigation inclusion of Marriott's Directors with claims of violating the securities law related to data breaches and claims of personal liability demonstrates that all firms are expected to monitor cyber risk and directors can be found liable if lack of oversight occurs.

These lawsuits, fines, and reputational damage could have potentially been avoided or more effectively managed if Marriott had identified this data breach during the acquisition due diligence process, prior to acquisition of Starwood.

Tool C

INSIDER THREATS

- OBJECTIVE OF THE TOOL
- WHAT IS THE INSIDER THREAT?
- QUESTIONS BOARDS SHOULD ASK SENIOR MANAGEMENT ABOUT INSIDER THREATS

OBJECTIVE OF THE TOOL

Mitigation of the insider threat poses one of the greatest challenges to managing cyber risk. Precisely because the delivery of this threat involves leveraging the legitimate access of "trusted insiders" (employees, contractors, vendors, and others) to an organization's network, systems, and data, it can be harder to detect than other threats in which the forensic indicators of compromise are more immediate and obvious. This tool defines the insider threat and outlines the categories of insider incidents and the types of insider threat actors. Finally, it proposes questions that boards should be asking to ensure executive management is adequately addressing insider threats.

WHAT IS THE INSIDER THREAT?

ENISA defines an insider threat is an action that may result in an incident, performed by someone or a group of people affiliated with or working for the potential victim. Insiders may cause harm unintentionally through carelessness or because of a lack of knowledge. Since these insiders often enjoy trust and privileges, as well as knowledge of the organisational policies, processes and procedures of the organisation, it is difficult to distinguish between legitimate, malicious and erroneous access to applications, data and systems[1].

The objectives of insider attacks can result in the following forms of harm to an organization:

* Sabotage
* Fraud
* Intellectual property theft
* Espionage
* Loss of share value
* Loss of consumer confidence

Insider attacks are generally carried out through the following types of actors:

* Careless or negligent employees
* Disgruntled or departing employees
* Malicious insiders
* Inside agents (witting or unwitting)
* Third-party partners

1 ENISA, "Insider Threat Landscape 2020", 2020, https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/etl-review-folder/etl-2020-insider-threat.

TOOL E

QUESTIONS BOARDS SHOULD ASK SENIOR MANAGEMENT ABOUT INSIDER THREATS

Boards should start by understanding the possible risk associated with insider threats.

* What are the top risk scenarios involving insider threat?
* What is our probable loss exposure related to the insider threat scenarios?
* What are the most effective controls and which ones should be prioritized?

Boards can follow-up with more detailed questions regarding the company's practices to defend against insider threats:

* Does the company have a documented insider threat mitigation plan with clearly designated oversight, management, and reporting responsibilities?
* Does the company have a whistleblowing7 or other mechanism that could be easily used to report suspected or detected insider threats?
* Who are the appropriate stakeholders to involve in the insider threat mitigation plan within the organization—information security, physical security, general counsel, human resources, corporate investigations, privacy, etc.?
* What manual and automated systems are in place to vet employees and identify anomalous, negligent, and/or malicious behaviour throughout the employee lifecycle?
    - Background checks during recruitment and hiring process and during an employee's tenure
    - Onboarding procedures
    - Continuous monitoring
    - In-service training
    - Employee reporting mechanisms
    - Secure off-boarding procedures
    - Data usage logs
    - Authorization and access rights controls
* Is access to company facilities, data, and systems properly aligned with each employee's respective job function (no more than necessary to perform their functions)? Does the organization have an overall identity and access management program?
    - What procedures are in place to ensure prompt adjustment of access privileges in the event of an employee's change in status (transfer, promotion, termination, etc.)?
    - What procedures are in place to detect and prevent activity which exceeds or otherwise falls out of scope with designated privileges? Is regular review implemented and enforced?
    - Is physical access to company space appropriately controlled to prevent unsanctioned removal of company assets, media, and/or data?

* Is there a data classification policy in place and enforced to ensure proper labelling and handling?
* Do respective employees with access to personal information comply with GDPR and local personal information regulation requirements? Do relevant documents confirming this exist?
* Do employees and coworkers all have non-disclosure clauses in their engagement contracts?
* Do contracts with vendors and third-parties include such clauses?
* Is there a comprehensive incident response plan in place involving all stakeholders (human resources, general counsel, compliance, security, and others) in the event of an insider incident?
    - Does it align with other internal incident response frameworks?
    - Are there in-house forensic capabilities, or is an outside firm on retainer?
    - Do appropriate relationships currently exist with law enforcement partners to assist with the response?
    - Do appropriate relationships exist with regulators that may require reporting about such incidents?
* Does the company have a backup and recovery program? Could the company recover its systems and critical data if access was prevented, or data corrupted in the main system?
* Does the company have strong controls around critical vendor relationships to prevent unauthorized access?
    - How are third-party vendors monitored to control unauthorized access?
    - For third-party cloud and software-as-a-service providers that are critical to business processes, what controls are in place to prevent unauthorized access while also enabling the business? (Reference Tool D for Third-Party Risks and Tool K Securing the Cloud for more in-depth practices, controls, and questions.)
* How does the company measure the effectiveness of its insider threat mitigation plan?
    - Does the company periodically test the plan with internal assets and external parties to validate its effectiveness?
    - Does the company insider threat mitigation plan maintain procedures to properly document incidents or insider threat activity?
    - Does the company maintain metrics to identify and analyse patterns of insider threat activity to assist with reducing vulnerability?
* Does the company have adequate programs in place to sensitize employees to insider risks and train them to detect, report, and mitigate potential incidents?
    - Do we have a security awareness program in place?
    - Are we tracking metrics of this program to identify progress or problem areas?
    - Is there a disciplinary or continuing education framework for employees failing tests? Does it show improvement in employee behaviour?

Tool D

SUPPLY CHAIN AND THIRD-PARTY RISKS

- SUPPLY CHAIN AND THIRD-PARTY RISK MANAGEMENT QUESTIONS
- CASE IN POINT

The strength of an organization's cybersecurity can be completely undermined by the weakest link in its supply chain. At stake may be the company's profitability, reputation, and credibility.

Recent research highlights a 300 percent increase in supply chain cyber-attacks in 2021 compared to 2020 levels. For instance, attackers in the high-profile 2021 SolarWinds breach made use of these tactics to target many SolarWinds customers, dozens of them in the Fortune 500. In an increasingly interconnected digital ecosystem, boards and cybersecurity leaders must prioritize addressing these risks to achieve true resilience.

Successfully competing in the digital age may require using a long and possibly global supply chain, including the use of third-party technologies and software. While this business practice may generate strong economic advantages these benefits need to be balanced with recognizing and overseeing potential security risks. A 2019 conference for directors on cybersecurity concluded that one of its key takeaways was that directors must, "remain familiar with the company's processes to identify, assess, and manage third-party and supply chain risks[1]."

This tool details questions that directors should be asking management to ensure adequate security measures are in place to address supply chain risks.

SUPPLY CHAIN AND THIRD-PARTY RISK MANAGEMENT QUESTIONS

1. How do we balance the financial opportunities (lower costs, higher efficiency, etc.) created by greater supply-chain flexibility with potentially higher cyber risks?

2. How much visibility do we currently have across our supply chain regarding cyber risk exposure and controls? Which departments/business units are involved? Is it clear who are authorized to provide supply chain partners business sensitive data such as product, financial or person data?

3. What will need to be done to fully include cybersecurity in current supply-chain and vendor/third-party risk management?

4. How are cybersecurity requirements built into contracts and service-level agreements?How are they enforced? Are our contracts and service-level agreements written to include requirements for the following:

    a. Written cybersecurity policies.

    b. Personnel policies, such as background checks, training, etc.

    c. Access controls.

    d. Right to use, re-use, modify, store, distribute data

    e. Obligations to return, remove or purge data

    f. Encryption, backup, and recovery policies.

    g. Secondary access to data.

    h. Countries where data will be stored.

    i. Notification of data breaches or other cyber incidents.

    j. Incident-response plans.

1 Stephen Klemash, "What boards are doing today to better oversee cyber risk", EY, 16 July 2019, at: https://www.ey.com/en_us/board-matters/what-boards-are-doing-today-to-better-oversee-cyber-risk (August 6,2019)

k. k. Top cyber risk assessment.

l. l. Audits of cybersecurity practices and/or regular certifications of compliance

5. How difficult/costly will it be to establish and maintain a viable cyber vulnerability and penetration testing system for our supply chain?

6. How difficult/costly will it be to enhance monitoring of access points in the supplier network?

7. Do our vendor agreements bring new legal risks or generate additional compliance requirements (e.g., FTC, HIPAA, CCPA, GDPR, etc.)?

8. Are we indemnified against security incidents on the part of our suppliers/vendors?

CASE IN POINT

An Impact on the Consumer Experience

A US-based consumer reporting agency suffered a data breach that affected the personally identifiable information of more than 100 million Americans. Hackers penetrated the company's information system using known vulnerabilities in licensed software, which was developed by a third-party software vendor and widely used. An external third-party notified the public about vulnerabilities before the breach[2]. The data breach would have been preventable had the company patched the vulnerability in the third-party software. The company was required to pay a multimillion-dollar data breach settlement that was paid out in 2022 to affected customers.

Ransomware Attack Disrupts Global Supply Chains

Despite being warned by researchers of their software vulnerabilities, in 2021 a major US IT management firm suffered a ransomware attack on its virtual system administrator (VSA) software.

Although the company initially said that only 0.1 percent of its clientele had been affected, the company's software was used by large IT companies that offered services to hundreds of small- and medium-sized businesses

(SMBs). As a result, the company told nearly 40,000 customers to disconnect their services. Given the large network created through managed service providers (MSPs), nearly 1,500 businesses—predominately SMBs—had their operations disrupted worldwide with ransomware. The attack—arguably the largest ransomware attack yet—was successful in disrupting global supply chains over the long Independence Day weekend[3].

2 Lily Hay Newman, "All the Ways Equifax Epically Bungled Its Breach Response," Wired, September 24, 2017

3 Gerrit De Vynck and Rachel Lerman, "Widespread ransomware attack likely hit 'thousands' of companies on eve of long weekend" The Washington Post, July 3, 2021. https://www.washingtonpost.com/technology/2021/07/02/kaseya-ransomware-attack/.

Case Study: Major Airline Responds Quickly to Third-Party Vulnerability

In 2018, a major airline revealed that some consumer information had been compromised via a vulnerability in a third-party online chat support service. In response to this breach, the airline launched a custom website outlining details of the breach and implemented a comprehensive communications campaign highlighting education and best practices. The airline also worked with partners to analyse the breach, including identifying whether the vulnerability had impacted any of the airline's own website or its own computer systems. Once the airline had successfully managed the fallout from the breach, the airline filed a lawsuit against the third-party service citing that the third-party vendor had failed to comply with a contractual promise to notify the airline immediately should a breach occur[4].

4 Delta, "Updated Statement AI-Cyber incident", 2018 https://news.delta.com/updated-statement-247ai-cyber-incident;https://blog.radware.com/security/2018/10/the-delta-airlines-security-breach-a-case-study-in-how-to-respond-to-a-data-breach/; Fast Company, "Delta Air Lines just revealed a serious data breach: Here's what you should do next", Christopher Zara, 2018 https://www.fastcompany.com/40554759/delta-air-lines-just-revealed-a-serious-data-breach-heres-what-you-should-do-next

Tool E

INCIDENT RESPONSE

- OBJECTIVE OF THE TOOL
- CASE IN POINT
- WHO TO CONTACT AFTER A CYBERATTACK
- QUESTIONS BOARDS SHOULD ASK SENIOR MANAGEMENT ON INCIDENT RESPONSE

OBJECTIVE OF THE TOOL

Since not all incidents can be prevented, response is a critical component of a cybersecurity program. Having incident response capability is necessary for all organizations regardless of size or sector as virtually all organizations are now targets of cyber-attack. This Tool outlines steps boards should take to ensure that their organizations have an effective incident response program.

The business capabilities and functions required to support incident response are:

* **Governance:** Knowledge of assets and where they reside with appropriate controls, data protection, and regular risk assessment and management, policies, and procedures
* **Protective Capabilities:** Policies, employee awareness and education, control procedures to validate access, information protection procedures, and continual validation
* **Detection Capabilities:** Set of capabilities to detect anomalies and events, and continuous monitoring for effectiveness
* **Response:** Response playbook; regular cyber exercises; coordinated efforts across technology teams, business, legal, communication, and law enforcement
* **Recovery:** Speedy remediation and after-action improvement

INCIDENT RESPONSE – THE "HOW" MATTERS

While the research remains inconclusive, there is evidence that the mere act of disclosing a cybersecurity related incident can impact a company's share price and reputation. However, the experiences of some organizations in responding to large-scale breaches have demonstrated that how a company responds to an incident can correlate and contribute both positively and negatively to its brand reputation and stock valuation.

CASE IN POINT

International Aluminium and Energy Company: *Ransomware targeted an industrial company. Files were encrypted across multiple systems and locations, thus halting some of the company's production.*

Financial Impact: *~$75 million USD*

Company Response: *Came forward publicly quickly after the breach occurred. Very quickly put incident response plans into action, had good backup and didn't have to pay ransom. It segregated networks to prevent the spread of the infection.*

Result: *Stock price went up 1.5 percent despite loss of productivity.*

TOOL E

WHO TO CONTACT AFTER A CYBERATTACK

* Data forensics investigation team. Within your organization this group may be called an incident response team or digital forensics team. Successful security programs may include internal teams and third-party incident responders on retainer.

* Law enforcement and regulators (International, EU level, local law enforcement, ISACs, CSITs/CERTs, FBI/Interpol, EUROPOL, ENISA, etc.)

* Insurance carrier

* Customers

* Businesses that might have been affected

* Your bank, credit bureaus, financial services partners

QUESTIONS BOARDS SHOULD ASK SENIOR MANAGEMENT ON INCIDENT RESPONSE

These questions will help boards of directors ask senior management the right questions to ensure that incident response and supporting capabilities can withstand a cyber incident and create a speedy path to business service recovery and a timely response to customers and the market.

1. **The Incident Response Plan (IRP)**

   I. Is there a clear incident playbook with definitions of roles, responsibilities, processes, and communication lines between business units and the company as a whole? For publicly traded companies, is there a clear method outlined and practiced for assessing, determining, and disclosing materiality of an incident?

   II. How is the incident response plan being tested and then updated, based on results from reports, exercises, and simulations?

   III. How is the incident response plan measured against the risk appetite of the company's overall business plan?

2. **Communication and Authority**

   I. What are the escalation criteria for notifying senior leadership and the board?

   II. Who has the final decision-making authority within each business unit and among senior leadership on how to respond during an incident?

   III. How is the feedback mechanism to higher management organized relative to the importance of specific systems for day-to-day operations?

3. **Exercises and Simulations**

   I. Are there organizational resiliency tests using large risk scenarios through tabletops exercises, common threat simulations, and penetration testing?

   II. What is the frequency of table-top exercises? When do these occur, and are they general or attack specific?

   III. Are our HR and PR responses also being accounted for within exercises and simulation?

4. **Information Sharing**

   I. Are there established relationships in place with the intelligence community, relevant law enforcement, and key regulators (CSIRTs/CERTs)?

   II. Who has the task of maintaining a relationship with relevant governmental agencies?

   III. Have information-sharing relationships been established through information sharing and analysis centres (ISACs) and consortiums and with other companies?

5. **Compliance and Reporting**

   I. Does the organization have notification and mandatory reporting obligations (e.g., regarding different regulations of EU, like the General Data Protection Regulation, etc.)?

   II. Who holds the highest authority within the organization in verifying that our incident response accounts for regulatory requirements?

   III. How are we maximizing our ability to share incident report data with our competitors and the regulators without disclosing any confidential company data?

6. **Disclosing Incidents**

   I. What are the criteria and what is the process for disclosing incidents to investors?

   II. How can we represent not only the cyber incidents but also the effectiveness of our incident response in our quarterly report or other relevant documents?

   III. What is our specific plan to disclose a disruption both internally and externally?

7. **Mitigating Losses**

   I. What can we do to mitigate the losses from an incident?

   II. Does senior management know who has the authority to swiftly disable large groups of machines or servers if they are infected by malware?

   III. What reporting mechanism is in place to ensure we are investing sufficient resources into our data recovery capacity?

8. **Measuring Incident Response Effectiveness**

   I. What are the critical, key performance indicators used to measure incident response effectiveness (e.g., time to detect and time to respond)?

   II. What kind of meta-data monitoring, collecting, and reporting mechanism is in place?What is the cost of this mechanism, and what benefit has it returned?

   III. Do we simulate how long a recovery procedure would take and what kind of cost the business would incur?

9. Post-Incident Response

I. What key steps do you follow after a critical incident?

II. What steps do you follow to ensure this type of incident doesn't occur again?

III. How are we educating our employees to be more aware of our policies, procedures, and reporting mechanisms?

IV. Do we require a post-mortem evaluation based on findings of the forensics investigation as part of the incident response plan?

CASE IN POINT

POOR INCIDENT RESPONSE

Poor incident response to a cyberattack can be characterized as vague and downplayed media responses to a hacking event, which merely stimulates questions and fear among company customers and the general public. The progression of one such event follows:

* *A hacker organization conducted a cyberattack on a third-party service company, gaining access to a computer that contained customer information of its lead providing company, an identity and access manager*[1].
* *After five days of access, from January 16–21, 2022, the providing company discovered the breach and closed off access. The hacker organization informed the public of the data risk to the customers due to the cyberattack two months later, on March 22, 2022. The providing company held their response to the occurrence until a week later, on March 29, 2022*[2].
* *The provider apologized for notifying its customers late*[3].
* *After investigation, the provider reported that the damage was not vast, doubling down on the fact that transparent customer communication is vital even after "small" attacks*[4].
* *The provider then cut off all ties with their third-party processing company*[5].
* *A year after the report of the cyberattack, the provider then found itself to be the recipient of a class-action lawsuit, due to the small attack possibly impacting 366 corporate clients (2.5 percent of its customer base)*[6]

1 Osborne, Charlie, "As Lapsus$ comes back from 'vacation,' Sitel clarifies position on data breach", 2022, ZD Net. Retrieved from: https://www.zdnet.com/article/as-lapsus-comes-back-from-vacation-sitel-clarifies-position-on-data-breach/

2 Faife, Corin. 2022. "Okta sys security protocols limited hack, but response came too slow" The Verge. Retrieved from https://www.theverge.com/2022/3/23/22992894/okta-hack-cso-security-protocol-sitel-lapsus; Kan, Michael. 2022. "Okta Says Hack From LAPSUS$ Group May Have Ensared 366 Brands" PC Magazine. Retrieved from https://www.pcmag.com/news/okta-says-hack-from-lapsus-group-may-have-ensnared-366-brands

3 Tung, Liam. 2022. "Okta: We made a mistake over Lapsus% breach notification." ZD Net. Retrieved from https://www.zdnet.com/article/okta-we-made-a-mistake-over-lapsus-breach-notification/

4 Faife, Corin, 2022. "Okta sys security protocols limited hack, but response came too slow" The Verge. Retrieved from https://www.theverge.com/2022/3/23/22992894/okta-hack-cso-security-protocol-sitel-lapsus

5 Lemos, Robert. 20222. "Okta Wraps Up Lapsus$ Investigation, Pledges More Third-Party Controls" *Dark Reading*, Retrieved from: https://www.darkreading.com/cloud/okta-wraps-up-lapsus-investigation-pledges-more-third-party-controls

6 The Gross Law Firm. (2022). "Shareholder Alert: The Gross Law Firm Notifies Shareholders of Okta, Inc. of a Class Action Lawsuit and a Lead Plaintiff Deadline of July 19, 2022 – (NASDAQ: OKTA)" Cision PR Newswire. Retrieved from: https://www.keloland.com/business/press-releases/cision/20220608NY82425/shareholder-alert-the-gross-law-firm-notifies-shareholders-of-okta-inc-of-a-class-action-lawsuit-and-a-lead-plaintiff-deadline-of-july-19-2022-nasdaq-okta/; Gately, Edward. 2022. "Okta Data Breach Could Impact Hundreds of Corporate Customers" Channel Futures. Retrieved from https://www.channelfutures.com/security/okta-data-breach-could-impact-hundreds-of-corporate-customers; Barsky, Noah. 2022. "Okta's Fearful Cyber Response Worse Than Hackers' Peek - How 3 Tempting Tech Crisis Shortcuts Cost More" Forbes. Retrieved from https://www.forbes.com/sites/noahbarsky/2022/06/01/okta-fearful-cyber-response-worse-than-hackers-peek/?sh=222 740d05ab7

CASE IN POINT

GOOD INCIDENT RESPONSE

A good incident response will include a rapid incident response plan that acts to contain and prevent cyberattacks from occurring once an attack was detected. Additionally, a good response will illustrate the importance of public transparency of the cyberattack. A company that is attacked might even provide information about the tactics and techniques of their cyberattack. Although the monetary damage due to a company's cyberattack isn't clear (presumably because it was well-mitigated), company stock might decline when revealing a vulnerability, but this leads to only up to an average 4 percent drop with 40 percent of businesses stock prices unaffected. The impact of incidents is slightly greater, with stock that drops more than 5 percent, 63 percent of businesses recover in less than a month[7].

Summary:

* *A software provider effectively communicated with the public after a cyberattack by an infamous hacking organization, ensuring that the breach was minimal, with only a single employee account was compromised.[8]*
* *The provider stated that their cybersecurity team was on the case immediately after the hackers disclosed their attack and stated that the provider's cybersecurity experts were able to stop the hack mid-operation[9].*
* *The hacked company then shared information with the public regarding the tactics the hackers used to conduct their attacks[10].*
* *The software provider then revealed that their cybersecurity teams had been "studying" the hacking organization and the attack techniques that the hacker group had used in the past[11].*

7 Sheridan, Kelly. 2021. "Do Cyberattacks Affect Stock Prices? It Depends on the Breach" Dark Reading. Retrieved from: https://www.darkreading.com/threat-intelligence/do-cyberattacks-affect-stock-prices-it-depends-on-the-breach

8 Culafi, Alexander. 2022. "Microsoft confirms breach, attributes attack to Lapsus$" TechTarget. Retrieved from https://www.techtarget.com/searchsecurity/news/252515022/Microsoft-confirms-breach-attributes-attack-to-Lapsus

9 Swabey, Pete. 2022. "Microsoft confirms Lapsus$ breach and reveals hacking group's tactics" Tech Monitor. Retrieved from https://techmonitor.ai/technology/cybersecurity/microsoft-confirms-lapsus-breach-and-reveals-hacking-groups-tactics

10 Swabey, Pete. 2022. "Microsoft confirms Lapsus$ breach and reveals hacking group's tactics" Tech Monitor. Retrieved from https://techmonitor.ai/technology/cybersecurity/microsoft-confirms-lapsus-breach-and-reveals-hacking-groups-tactics

11 Microsoft. 2022. "DEV-0537 criminal actor targeting organizations for data exfiltration and destruction" Microsoft. Retrieved from https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfilt ration-and-destruction/

Tool F

BOARD-LEVEL CYBERSECURITY METRICS

- OBJECTIVE OF THE TOOL
- METRIC FOCUS AREAS
- STRATEGIC METRICS VERSUS OPERATIONAL METRICS

TOOL F

OBJECTIVE OF THE TOOL

Modern businesses are increasingly data driven.

Boards use metrics to help inform their strategic and oversight functions on finance, market competition, marketing sales, etc. Similarly, oversight of various forms of enterprise risk such as market risk, credit risk, and operational risk have also evolved and progressively moved from qualitative assessments to quantitative assessment. This Tool describes how the board can use metrics to assess the effectiveness of cybersecurity programs and offers advice on how boards can leverage them to conduct oversight of their organization's cybersecurity programs.

METRIC FOCUS AREAS

Boards should expect metric-based reporting to focus on strategic, operational, financial/economic, and benchmark figures.

<table>
<tr><th colspan="2">QUESTIONS ABOUT METRICS RELEVANT TO SPECIFIC BUSINESS PROGRAM</th></tr>
<tr><td>STRATEGIC METRICS

Directors should ask management about strategic metrics related to the company's approach to security and risk.
* Which strategic metrics are most critical to our organization?
* How are we measuring those security and risk indicators that have the greatest impact on our outcomes as an organization?</td><td>OPERATIONAL METRICS

Operational metrics provide little strategic context or information about performance and risk position.
* Operational metrics can still be helpful in assisting the board in understanding critical compliance issues and stimulating useful discussions about trends, patterns, and root causes, and benchmarking.</td></tr>
<tr><td>DEVELOPING CYBER ECONOMIC METRICS

Cyber risk is now an accepted board-level conversation. For boards to better understand cybersecurity data, it helps to translate the data into financial metrics. Directors will need to work with management to determine the most relevant information, given their organization's unique environment.</td><td>BENCHMARK DATA

Third-party benchmarking data can be useful for assessing performance against peers and within your industry.
* Most benchmarking data is operational and may not contain appropriate strategic context on its surface. Boards should ask management how this data applies back to the overall cybersecurity or organizational strategy.</td></tr>
</table>

CIBERSECURITY RISK MITIGATION CROSSES THREE FUNCTIONAL AREAS

ENTERPRISE IT	PRODUCT LINE	SUPPLY CHAIN
Risk managed by it with internal audit oversight:	***Risk managed by programs; security requirements defined by the customer:***	***Risk managed by supply chain risk management (SCRM) Team:***
* Intellectual property (IP) creation, including engineering systems, program file shares, software development pipelines * Financial data including Hyperion. PeopleSoft, SAP and spreadsheets * Personal Identifiable Information (PII) maintained in HR systems * Enterprise IT systems are the focus of emerging cybersecurity regulations and frameworks... NIST 800-171, CMMC, GDPR	* Classified vs unclassified * NIST 800-53 low, moderate, high * Risk Management Framework (RMF) * Risk of malware introduced into software build process (e.g., Solar Winds) * Risk of corrupt platform being delivered to the customer * Attacks against critical infra-structure that we maintain (e.g, FTI)	* Led by Supply Chain, includes En-terprise IT, Engineering, Industrial Security and Contracts * Goal is to ensure supply chain does not introduce a defect or malware that impacts delivery to our customers * Flo-down customer security requirements * Ensure compliance to cybersecu-rity requirements and our data is protected

Cybersecurity risk mitigation needs to address each area as failure in one can impact the other (e.g., Solar Winds), having far reaching effects. The IT Cybersecurity and Internal Audit teams address Enterprise IT Cybersecurity Risk.

STRATEGIC METRICS VERSUS OPERATIONAL METRICS

Directors should focus on strategic metrics about the company's approach to cybersecurity and risk that are provided by the company's management. While the focus should remain on strategic risks, certain operational metrics can be helpful in assisting the board in understanding critical compliance issues and stimulating useful discussions about trends, patterns, and root causes. Operational metrics can also be helpful with benchmark-ing when they help provide strategic context or information about the impact on business performance and strategic risk positions. It is the role of management to avoid using overly technical concepts and translate them in business impact terms that the board understands and can use as part of its oversight role.

This Tool outlines examples of more detailed questions board members should be asking management to en-sure proper metrics are being collected on the enterprise's cyber risk, grouped in 5 categories as outlined in Principle 5. Directors will work with management to determine the level of depth required, depending on each organization's size and circumstances.

1. What is the threat environment we face?

Cyber risk leaders should provide the board of directors with an understanding of the threat environment that the company faces. Examples of good questions to ask include:

* What are the top threats faced by our industry?
* How impactful have these threats been to our peers?
* How many cyber incidents has our company experienced in the last reporting period?
* Are there any new emerging threats that are affecting our business performance?(ex.: trends in ran-somware, zero-day-attacks, new attack patterns)
* Are our threat intelligence capabilities adequate and how do they compare to our peers?

2. What is our risk profile looking from the outside-in?

Boards should get an assessment of the company's security posture from independent sources. Questions that boards should ask are:

* What is our vulnerability rating as measured by one of the leading security rating vendors?
* How does our rating compare against the industry benchmark?
* What are the security ratings of our strategic partners and suppliers?
* What are the findings of the latest penetration testing performed by our external provider?
* How mature are our cyber risk management practices as assessed by a leading cyber consultancy?
* Are there any outside sources for assessing our security posture that we may not be including? What about our audit firm?

3. What is our cyber risk profile as defined by management?

Boards should expect management to provide metrics assessing the status and the performance of their cybersecurity program. Questions that boards can ask are:

* How are we performing against basic cyber hygiene compliance metrics related to the "five P's" (passwords, privileges access, patching, phishing, and penetration testing)?
* How mature are our cybersecurity practices as measured against list of established best practices? (ex.: ISO/IEC 27001, NIST CSF, NIST800-53, CIS Controls/NAS9933)
* What is the percentage of critical systems downtime and time to recover?
* What is the mean time to detect and remediate cyber breaches?
* What percent of our supply chain failed our cybersecurity assessment?
* Are these metrics acceptable or not? How are they trending? What are our target goals?

4. What is our cyber loss exposure in economic terms?

As cyber risk has emerged as one of the top enterprise risks for most companies, boards and regulators are increasingly expecting companies to assess the frequency and the materiality of cyber events, and to express cyber risk in financial terms, similarly to the other forms of enterprise risk. Questions that the boards can ask are:

* What are our company's key assets ("crown jewels") and how do we measure their value?
* What are the top cyber risks we have as a company?
* What is the probable frequency and the probable magnitude of these top cyber events?
* What cyber risk quantification model or models are we using to assess cyber risk?Have these models been independently validated?
* What are the forms of loss that we can experience, and how are we measuring and reporting on those losses? (productivity, response costs, replacement costs, fines and judgements, reputational loss)
* What is the level of risk that we can tolerate as a business and how are we tracking against it?

* Is our cybersecurity spending adequate given the threats we face and our risk appetite targets?

5. Are we making the right business and operational decisions?

The boards must understand the cyber risk implications of strategic business decisions, as they support digital growth or transformation initiatives. Good questions to ask can include:

* What is the cyber risk that we can incur in launching this new business initiative (such as the launch of a new digital product, moving to the cloud, etc.)?

* What processes have we established related to making cyber risk acceptance, cyber risk remediation, and cyber risk transfer decisions?

* What cyber risk scenarios should we mitigate with internal controls and which ones should we insure against?

* How much cyber insurance do we need? Does the proposed cyber insurance policy cover us adequately? How has the changing cyber insurance market impacted our risk exposure?

* What is the cyber loss exposure associated with the new company acquisition (where applicable?) *(Reference Tool G for more in-depth discussion of cyber risk oversight of mergers and acquisitions)*

* What is the return on investment for our cybersecurity program?

* Which key controls are most cost-effective? Which ones are the least cost-effective?Are there any (possibly older/outdated) initiatives eating up resources that would be better spent elsewhere?

Tool G

MERGERS AND ACQUISITIONS

- CYBERSECURITY CONSIDERATIONS DURING M&A PHASES
- WHEN IT COMES TO CYBER RISK ASSESSMENT, EARLIER IS BETTER
- STRATEGY AND TARGET IDENTIFICATION PHASE
- DUE DILIGENCE AND DEAL EXECUTION PHASES
- INTEGRATION PHASE
- CONCLUSION

TOOL 5

CYBERSECURITY CONSIDERATIONS DURING M&A PHASES

This tool reviews cybersecurity risks at key stages of a merger or acquisition transaction and provides suggested questions for board members to discuss with management at each stage.

Introduction

Over the past few years, numerous high-profile cybersecurity incidents have emerged during or after large mergers and acquisitions (M&A) deals. These incidents have raised concerns among corporate executives, investors, and regulators.

Corporate executives and M&A professionals will point to improved processes and outsourced services to identify and prevent security issues. However, despite heightened awareness and the existence of various vendors who can assist in the cybersecurity elements of the M&A process, the cyber risks for acquirers are only increasing. This is due to factors such as increased online connectivity within companies and with their suppliers and customers in addition to a more distributed workforce, digital transformation, and increased cloud adoption. All of the above serve to increase the attack surface, resulting in an elevated threat environment.

The decision makers in an M&A transaction often tend to approach the strategy, finance, legal, or operational risks before accounting for cyber risks. As noted by Rob Gurzeev of TechCrunch:

> *'With limited time and less priority on cybersecurity, M&A teams are inclined to focus on more "urgent" transactional areas of the deal process, including negotiating key business terms, business and market trend analysis, accounting, debt financing, and internal approvals. With an average of only 2-3 months to evaluate a transaction before signing, cybersecurity typically only receives a limited amount of focus.*[1] *It is probably not a coincidence that a recent poll of IT professionals by Forescout showed that 65%of respondents expressed buyer's remorse due to cybersecurity issues. Only 36% of those polled felt that they had adequate time to evaluate cybersecurity threats*[2].

Timely identification of cyber risks allows appropriate quantification of the valuation considerations, including estimated one-time and recurring costs to remediate cyber vulnerabilities or gaps in regulatory compliance. It also enables re-negotiation of deal terms that either build the cost of remediation into the arrangement price or provide for insurance or other means of claw-back if the identified vulnerability becomes an incident.

During each phase of the transaction, directors should expect to receive from management as much certainty and quantification as possible about the scale of inherited risks.

WHEN IT COMES TO CYBER RISK ASSESSMENT, EARLIER IS BETTER

Early investigation and identification of the target company's cyber posture and risks are critical during the M&A process. Surprisingly, a 2020 report by IBM shows more than half of surveyed companies do not perform their cybersecurity assessments until after the completion of due diligence[3]. In fact, the earlier that cybersecurity assessment takes place during the M&A process, the more comprehensive will be the remediation opportunities available to the acquirer.

1 Gartner Press Release, "Gartner Says the Average Time to Close an M&A Deal Has Risen More Than 30 Percent in the Last Decade", Gartner. October 15, 2019, https://www.gartner.com/en/newsroom/press-releases/2018-10-15-gartner-says-the-average-time-to-close-an-manda-deal-has-risen- more-than-30-percent-in-the-last-decade [accessed January 15, 2021].

2 Forescout Technologies, "The Role of Cybersecurity in Mergers and Acquisitions Diligence", Forescout Technologies. June 2019, https://www.forescout.com/company/resources/cybersecurity-in-merger-and-acquisition-report/ [accessed January 15 2021

3 Julian Meyrick, Julio Gomes, Nick Coleman, and Stephen Getty, "Assessing Cyber Risk in M&A: Unearth Hidden Cost Before You Pay Them", IBM Institute for Business Value. September 2020, https://www.ibm.com/downloads/cas/RJX5MXJD [accessed January 15, 2021].

When companies conduct a risk assessment, they should be aware that:

* A cyberattack may have already resulted in the loss of the target company's intellectual property, thus reducing the value of the company.
* A cyberattack that occurred prior to closing, regardless of when it was detected, could expose the acquiror to investigation costs, financial liability, regulatory penalties, or reputational damage.
* Attackers might still be in the acquiree's network, creating a risk of the attacker migrating into the acquiror's network.
* The acquired company may be targeted immediately after the announcement. Additionally, the subsequent integration of the acquiree's legacy systems or applications may introduce malware and or other vulnerabilities to the acquirer.

Directors should expect management to conduct a cyber risk assessment for each phase of the transaction life cycle to confirm systems and processes are secure, and to quantify the risks that may impact the company after the deal closes, impacting revenues, profits, market value, and brand reputation.

The table below outlines a few suggested questions that directors can ask members of management at each phase of the deal cycle. Further details are provided on the following pages.

TRANSACTION LIFE CYCLE PHASE	QUESTIONS FOR DIRECTORS TO ASK MANAGEMENT
Strategy and target identification	* Have we evaluated all relevant publicly available information on the target's cyber "history"? Possible sources include ratings, new stories, and publicly available regulatory filings. * What is the company's cyber-reputation as perceived by customers, suppliers, and other key stakeholders? * What is the range of potential financial impact of the identified cyber risks? * What cyber-related legal and regulatory requirements are applicable to the company?
Due dilligence and deal execution	* Have we conducted a detailed cybersecurity assessment?What did it cover? What were the findings? How did the findings stack up against our own standards? * What measures will we and other key parties (target company, advisors, etc.) be taking to guard against the risk of cyberattacks during the transaction process?
Integration	* What cybersecurity issues have arisen that were not previously identified? * What is the status of key milestone attainment? * Have our new employees been trained to our standards for cybersecurity?

The risk of attack may start even before an official offer or merger announcement is made[4]. Sophisticated attackers look for hints that a company is considering a merger, acquisition, or divestiture. They may be tipped off by industry chatter, a slowdown in a company's release cycle, staff reductions, or data leakage through social media channels.

The fact gathering in the earliest stages of the transaction should involve legal, corporate development, and security specialists. This process should identify and evaluate all relevant publicly available information on the target's cyber "history" including any disclosed or rumoured undisclosed breaches. By using analytics to monitor social media, the acquiror can also access real-time information on how a target's cyber reputation is perceived by customers and its marketplace.

During the strategy and target identification phase27, management should therefore gain an understanding of cyber risks associated with the target company and can perform the following analyses even before direct engagement with the target company:

Model the financial impact of identified cyber risks

Risk factors, vulnerabilities, and consequences need to be analysed and quantified. This should include cyber risk models that can reflect not only the impact on a company's return on invested capital, but also the results of loss of competitive advantages, costly remediation, fines, and possibly years of litigation, depending on what was stolen.

Understand the cybersecurity regulatory environment of the target company

Cybersecurity regulations at EU member level vary widely, and each industry faces an increasing number of separate regulators. Breaches of the European Union's Global Data Protection Rule (GDPR) can lead to potentially massive penalties (up to 4% of a company's revenues) representing a significant risk that boards should understand before moving forward with any acquisition involving access of data of European individuals.

The most fundamental step for managing information and privacy risks related to the transaction is understanding what types of data the target organization creates, receives, and collects as part of its business processes. As a starting point, companies should consider requesting the target's data inventory that identifies the types of data that are most critical to the target organization (e.g., intellectual property, financial documents), require special handling or protection (e.g., personal data), or are required by law or regulation (e.g., records). Organizations are increasingly using advanced text analytics and various artificial intelligence (AI) technologies to inventory and classify data. Search criteria and predictive analytics are established to explicitly identify types of data and where the data is stored.

Knowing what data the target organization holds is of limited use unless management also knows where it is. Devices that are commonly not identified include laptops and phones. Organizations that cannot efficiently locate personal data will be hard-pressed to demonstrate compliance with privacy regulations. Protecting the privacy of customer and employee data is impossible without appropriate technical and organizational security measures. The target should have controls in place to ensure that personal data is safeguarded from unauthorized access, processing, destruction, and damage.

Finally, the acquiror should understand the target's controls over disposition of data once it exceeds retention requirements and need not be preserved under any legal hold.

4 FRSecure, "Mergers and Acquisitions Cybersecurity Checklist", FRSecure, https://frsecure.com/mergers-and-acquisitions-cybersecurity-checklist/

During these phases, cybersecurity due diligence is critical[5]. Significant identified problems would call for negotiation of a reduction in purchase price to cover costs of necessary remediation. Depending on the risks identified, the board may request that management address identified matters through a transitional services arrangement with each party's responsibilities clearly identified; may defer approving the transaction until remediation is complete; or may decide to back out of a transaction if the identified risks are too great to scope or assume. Due diligence teams can identify cyber risks by conducting a tailored cybersecurity assessment designed to identify:

* Insufficient investments in cybersecurity infrastructure, as well as deficiencies in staffing, policies, etc.
* Lax cultural attitudes toward cyber risk.
* Cybersecurity-related terms and conditions in customer and supplier contracts that have a potential financial impact or that could result in litigation for noncompliance.
* Noncompliance with cybersecurity-related data privacy laws or other applicable regulations and requirements.
* Recent data breaches or other cybersecurity incidents.

The acquiror's assessment would review the security architecture, conduct forensic analysis on key network devices, and review logs looking for any indication the target might already be compromised. It should also include a review of recent or ongoing breach responses, tools, policies, and regulatory positions to identify security gaps, risks, and potential liabilities.

Acquirors may consider establishing a contingency fund to be held in escrow for potential exposures that may occur after closing. Where there has been a recent breach, the assessment should also reveal if the target has appropriately remediated to prevent a recurrence. Boards should not, however, assume that on-site assessments are guaranteed to identify all deficiencies. The nature of due diligence means the assessment team may not be given access to interview key security personnel who are not aware of the potential acquisition. Additionally, the assessment represents only a snapshot in time and may well lack historical context of past issues.

Prioritization will certainly be a necessary key judgment. Some issues may need to be addressed immediately if the acquired company is going to be integrated within the short term. If the entity is to be run as a separate, wholly owned subsidiary, however, the target's risks may potentially be "quarantined."

Acquirors should fully understand the target company's requirement for domestic and global compliance and reporting. The acquiror must not only understand any new regulatory requirements, but must also demand information on any recent, current, or anticipated engagements with regulators due to cyber incidents.

Acquirors should consider conducting "dark web" (anonymously run and difficult-to-access websites favoured by hackers) searches about the target, their systems, data, and intellectual property. This helps identify whether the company is already on attackers' radars, whether its systems or credentials are already compromised, or whether its sensitive data is for sale or being solicited.

Acquirors should also consider engaging vendors specializing in researching malware infections to look for infections in the target company and for any holes in their defences that are visible from the outside. This cybersecurity hygiene-related information is publicly available and can be used to compare one company to another, allowing management to save time and energy by not pursuing companies whose risk profile is unacceptably high.

5 Stuart Davis and Marko Polunic, "The Critical Role of Cybersecurity in M&A: Part 1, Due Diligence", Crowdstrike. October 20, 2020, https://www.crowdstrike.com/blog/role-of-cybersecurity-in-mergers-and-acquisitions-part-1/ [accessed December 22, 2020]

Evolution in the legal landscape must be taken into account for effective due diligence. For example, the upcoming NIS 2 directive on cyber security includes submit an early warning without undue delay and in any event within 24 hours of becoming aware of a significant incident. That early warning should be followed by an incident notification. The entities concerned should submit an incident notification without undue delay and in any event within 72 hours of becoming aware of the significant incident, with the aim, in particular, of updating information submitted through the early warning and indicating an initial assessment of the significant incident, including its severity and impact, as well as indicators of compromise, where available. A final report should be submitted not later than one month after the incident notification (or at least a progress report at that time in the event of an ongoing incident and a final report within one month of their handling of the incident). Understanding the acquiree's processes for incident reporting may help determine if such a timeframe would be achievable.

After the public deal announcement and before close and subsequent integration, new threats may emerge. Malicious actors know that there will be security audits in this period and an associated granting of temporary network access to outsiders. They may look to take advantage of the situation to penetrate networks in this period.

INTEGRATION PHASE

Once the organization has made the decision to acquire, it needs a plan to remediate compliance concerns, address risk exposure, and integrate security operations— where appropriate. This starts with a consolidated technology, security, and operations roadmap.

Acquirors should consider the merits of maintaining discrete operations with separate business and operating models. If the assets of the target will merge with core business operations, then integration is called for. Aside from traditional post-deal integration challenges related to people, processes, systems, and culture, an additional cyber risk accrues to both companies on the day the deal is announced. On Day 1, they become a target for social engineering attacks by those seeking to use the acquiree as a back door into the parent. Attackers will also seek to take advantage of the inconsistencies that exist between the platforms and technology operations of the two companies. The sooner the parent company can integrate the target company into their security environment, the better.

Many integration activities are complex and could take a year or more to complete. Integration teams need to have the cyber expertise to address:

* Security gaps identified during preceding phases
* Prioritization of remediation activities based on potential impact of identified gaps
* Prioritization of integration activities
* Employee training on newly integrated systems

Over the first six months post integration[6], boards should pay particular attention to integration project milestones slipping due to lack of funding, which is often a result of overly optimistic cost estimates. Such underestimation is common when estimates are created from incomplete knowledge inherent in a closely held due diligence process.

6 Stuart Davis and Marko Polunic, "The Critical Role of Cybersecurity in M&A: Part 3, Post-Close", Crowdstrike. November 12, 2020, https://www.crowdstrike.com/blog/role-of-cybersecurity-in-mergers-and-acquisitions-part-3/[accessed December 22, 2020]

However, there must also be a Day 1 integration plan to extend as much of the acquiror's cyber protections as possible to the target company immediately. At a minimum, the plan should include these steps:

* An exchange of threat information to include Internet domains to be blocked
* Employee awareness training emphasizing the risk of phishing attacks mimicking emails from the new parent company and other new risks. As companies combine their IT departments, hackers may use this time to impersonate administrators.
* A much deeper on-site assessment to further refine risks and integration costs
* Re-engagement with the open-source research vendors recommended during due diligence to identify spikes in indicators of cyber risk—a sudden increase in hygiene-related traffic after an announcement could be an indirect measure of other malicious activity
* Ideally, routing the target company's email through the parent company's email screening process if that capability exists

During this phase, it is also important to perform an operation-focused gap analysis to determine if one company has certain cyber capabilities or processes that the other does not have or that the combined organization could benefit from long term. If this is the case, the transaction is an ideal time for business changes or transformational activities to add value to the combined organization.

Acquirors should consider the benefits of leveraging cloud services to integrate the combined companies' applications and data faster. This can result in more rapid realization of synergies, less reliance upon third-party services, and potentially a reduction in overall risk through an organization hosting its own data applications.

CONCLUSION

Cybersecurity diligence during M&A calls for a two-pronged approach. Companies must conduct rigorous due diligence on the target company's cyber risks and assess their related business impact throughout the deal cycle to protect the transaction's return on investment and the entity's value post-transaction. In addition, all parties involved in the deal process need to be aware of the increased potential for a cyberattack during the transaction process and should vigilantly maintain their cybersecurity efforts. Applying this two-pronged approach during M&A will serve to ultimately protect stakeholder value.

Tool H

BUILDING A RELATIONSHIP WITH THE CISO

- INTRODUCTION
- UNDERSTAND THE CISO'S ROLE AND MANDATE
- SPEND TIME WITH THE CISO AND THE CYBERSECURITY TEAM OUTSIDE OF THE BOARD ROOM
- ASSESS THE CYBERSECURITY CULTURE
- DEEPEN THE RELATIONSHIP: MAKE THE CISO A STRATEGIC PARTNER

INTRODUCTION

As corporate information security functions mature, board directors must ask themselves how they can effectively communicate with the security team. The individual occupying the lead position, typically the chief information security officer (CISO), manages vast numbers of operational, reputational, and monetary risks. The scope and importance of the CISO's work behoves directors to form a candid relationship with this functional leader in the interest of performing effective cyber risk oversight. Accordingly, many board members are establishing an ongoing relationship with the CISO through full-board and committee meetings, but also outside the board room.

Different organizations and business processes require unique strategies and assessment depending on inputs like size, industry, value, risk tolerance, and threats. To help the board assess risk the CISO should have clear and consistent communication with the board that conveys the health and maturity of the cybersecurity program and calibrates risk tolerance for the corporation. This will also help the CISO effectively manage cybersecurity governance, performance, and risk management.

Strong working relationships with the CISO and their cybersecurity team goes hand-in-hand with establishing a strong culture of cybersecurity throughout the company—and including within the board itself. Having a visible relationship between the board and the CISO makes it very clear to the whole company that cybersecurity is worthy of their time. Today's CISOs need to be much more than just technical specialists in "security." To be effective, they need to be program managers, people developers, relationship builders, culture leaders, risk managers, strategists, industry luminaries, and growth oriented.

This tool offers guidance on how boards can more effectively establish a relationship with their organization's CISO and security team in order to establish an agreed-upon risk tolerance profile for the organization and assist in defining a requisite culture of cybersecurity. The questions below are stated as if a board member were asking the CISO a question. Most questions are followed by a bullet explaining the "why" behind the question to be asked. Because not every question will have relevance for every organization, directors should select those most appropriate to the issues and circumstances at hand.

UNDERSTAND THE CISO'S ROLE AND MANDATE

To build an effective relationship, the board needs to understand what the CISO does, what challenges they are facing, and what resources and support they have available to most effectively meet the needs of the corporation.

* What is your charter and scope of authority in terms of resources, decision rights, budget, staffing, and access to information? How does this compare to leading practice in our industry and generally?
    - Answers to these questions will help the director asking the question, and the board, establish a strong understanding of the CISO's role and the tools they have at their disposal to effectively manage cybersecurity risk. That's the first step in relating to them, building advocacy and trust.
* Who are you reporting to now, and has that changed in the past five years?
    - There is no clear industry consensus on this topic. By far, the largest percentage report to the CIO although there is a growing perspective (echoed earlier in this publication) that reporting to the CIO might not be the right answer. It is certainly true that a CIO might well have a conflict of interest between IT service delivery pressures, cost, customer experience, and security. Those factors need to be weighed against the value of having the CISO's supervisor being able to understand the technology and business risks and being capable of arbitrating trade-offs without escalating issues to the CEO for resolution. Some technology-oriented companies are now having the CISO report to the chief technology officer (CTO) to help ensure that cybersecurity is not just another risk management issue but is also more directly incorporated into product development lifecycles and portfolio strategies, frequently as a differentiator among the company's market competitors. Ultimately, the age-old tension between user experience and security remains regardless of whom the CISO reports to, and an enlightened CISO understands that all solutions need to be both safe

and performant. A key consideration for CISO reporting lines is whether or not that person has a strong voice on the executive leadership team to advocate appropriately for security. If the person representing the CISO at the executive level cannot influence the CEO and CFO, a security program cannot succeed.

* How is the organization's cybersecurity budget determined? What is its size and how does this figure compare with leading practice in a company's particular industry and generally? Is the level of funding aligned to the desired performance maturity for the information security program? Is the level of funding commensurate with the expected risk profile for the company?

    - Comparing these figures with industry spending trends is probably the best way to understand the adequacy of funding. CISOs will not typically ask the board for funding—that is a responsibility for management to address—but directors can certainly do their homework to understand whether or not the CISO's role can actually be effective given the funding levels provided by the organization and influence the CEO and CFO as required.

* How much of the security infrastructure is outside of your budget or directive authority as CISO?

    - Threats always evolve faster than the budget cycle. If a CISO is in the position of frequently asking others in the IT organization to upend their annual plans to accommodate emerging security needs, the chances of the changes being rejected are increased. Conversely, the more the CISO is in a position to make budget trade-offs internally in real time, the more rapid the response and the lower the risk. This situation is particularly true outside upper management where the lines of business frequently have more decision-making authority for product security trade-offs. For this reason many leading organizations are approaching cyber risk budgeting on a team basis as opposed to strictly as part of the IT budget.

* Which security tools or other investments were below the "cut" line in the budget?

    - Management is always eager to tell a board what they are doing but are less eager to discuss what they are not doing. A conversation about what fell below the cut line and what decision process was used to evaluate trade-offs will always be illuminating. This conversation should be anchored in planned risk-reduction initiatives and maturity roadmaps for appropriate decision calibration. Directors should be cautious about putting the CISO into a difficult spot with their CEOs and CFOs regarding spending decisions but should certainly consider asking questions about how priorities are being resourced and in what time frame. The CISO will likely consider the board as an ally in building consensus on critical priorities, which will build trust and strengthen the relationship versus putting the CISO in an awkward position of pointing any fingers at the CEO or CFO for failure to fund a critical security project that is aligned to a key enterprise risk reduction initiative[1].

* What role do you, as the CISO, play in the organization's enterprise risk management (ERM) structure and in the implementation of ERM processes?

    - Directors should probe to see if the CISO is just a contributor to the ERM process, or if they are part of the adjudication and risk decision making.

* What role, if any, do you as CISO play beyond setting and enforcing cybersecurity policies on the enterprise network and related control systems?

    - For example, does your CISO hold accountability for adjudicating cybersecurity risk associated with the organization's brand?

* As CISO do you provide input on the development process for new products, services, and systems? How about on the design of partnership and alliance agreements, etc., such that cybersecurity is built in rather than added on after the fact?

    - Your CISO's answer will be revealing about the extent to which the information security program is operational within the lines of business applications.

1 See, for example, Marc van Zadelhoff, Kristin Lovejoy, and David Jarvis, *Fortifying for the Future: Insights from the 2014 IBM Chief Information Security Officer Assessment* (Armonk, NY: IBM Center for Applied Insights, 2014).

* As CISO do you have a role in evaluating the cyber risk of acquisitions during due diligence?How about in the acquisition of new products or development of new business strategies—are you able to state strategic concerns about supply chain cybersecurity during discussions about those decisions?
    - Whether the company is acquiring another business fully entering into a new business agreement to acquire new software, CISOs should be involved in vetting cyber risk.
* Does the CISO get invited to meet with key external customers to either support a sales/capture activity or as a trusted advisor to the customer on matters of cybersecurity?
* How strong are your relationships among the c-suite and the executives and leaders of other key business functions in the company?

SPEND TIME WITH THE CISO AND THE CYBERSECURITY TEAM OUTSIDE OF THE BOARD ROOM

With packed board meeting agendas, it is unrealistic to think that the board can get sufficient insight into a company's cybersecurity posture through quarterly presentations. Board members should arrange to visit the security team and receive orientations firsthand from personnel situated on the front lines of cybersecurity. These sessions will provide valuable insights and learning opportunities for board members far beyond what they could obtain from highly scripted board presentations. The security team will appreciate it too, since visits like this can increase its visibility, raise morale, and reinforce the need to focus on this area. The board's greater familiarity with the team's mission and key security leaders will pay huge dividends when a crisis occurs. A crisis is the wrong time for directors to get acquainted with the CISO and key staff, their programs, and their relationship network across industry, customers, suppliers, and partners that may be able to help.

* Many security teams routinely produce internal reports for management and senior leadership on cyberattack trends, incidents, and threats. Directors can discuss with the CISO, corporate secretary, and board leaders whether this information might be relevant and useful to include in board materials.
* CISOs spend a great deal of time assessing risk, building threat models, and conducting exercises to test the effectiveness of cybersecurity controls. This is a great area for directors to engage the CISO and their team outside of the board room to directly deepen their engagement but also to indirectly learn about potential future business risks that might not normally come up during a more formal briefing to the board.

CISO as Compliance Czar?

All CISOs have to become compliance experts, but nobody really likes talking about compliance! Engaging the CISO to better understand the cyber regulatory landscape that the business is facing is one way to wade into that conversation and deepen the relationship with the board. In the EU and other places around the globe, there is increasing cybersecurity legislation that has to be considered, understood, influenced, and addressed tactically and strategically across the enterprise. The CISO should be conversant in these regulations and how their team is working to build compliance into other security practices. For more on the nuances of compliance, review Principle 2.

ASSESS THE CYBERSECURITY CULTURE

CISOs and their security teams occupy one of the most high-stress positions in an organization[2]. In many companies, the threat never really stops so there is an expectation of being available 24/7/365. Too often these cybersecurity teams do not receive adequate internal support and are blamed when there are system failures or performance issues that they did not cause. Low morale not only leads to high turnover—frequently it also leads to lower efficiency and increased risk. Partnership and support is essential for a healthy environment where these highly skilled workers can be effective and thrive. Questions for CISOs aimed at assessing the cybersecurity culture follow.

* How does your broader team collaborate with other departments and corporate functions on cybersecurity-related matters?
    - The CISO's answers will indicate how fully the security function and other departments cooperate and coordinate, including with:
        - IT operations to ensure that service capabilities and business applications are both performant and safe;
        - business development regarding due diligence on acquisition targets and partnership agreements; provide reusable cyber capabilities if cyber is a key aspect of the bid;
        - internal audit regarding the evaluation and testing of control systems and policies;
        - human resources for cyber workforce strategy, organization-wide cybersecurity culture and training, and employee development;
        - technology development of cyber proof points for our own cyber products and capability requirements for research and development;
        - purchasing and supply chain regarding cybersecurity protocols with vendors, customers, and suppliers; and
        - legal regarding compliance with regulatory and reporting standards related to cybersecurity, as well as data privacy.
* What direct support do you receive from the CEO, CIO, and senior management team, or are they only called onto the carpet when something breaks or a major breach has occurred?
* How do you measure and/or track maturity?
    - Boards should not assume that high performing organizations track maturity in only one way; or that the measure of a mature cybersecurity program occurs by simply counting all the tools that they have deployed or how many people that they have on their team. Maturing cybersecurity programs focus not just on defensive technology, alerting, and incident response; they also focus on improving processes that help to incorporate standard cybersecurity practices throughout all of the critical business workflows and activities. They focus on talent, risk, and culture. They have a mindset of continuous improvement and innovation. The board can tap into this understanding to help build synergy and partnership with the CISO on moving the needle on key enterprise risks.
* Do you or the information security team participate in cybersecurity information-sharing initiatives (e.g., industry-focused, cyber-community-focused, or public-private partnerships)?How is the information that is gathered from participation in such initiatives used and shared within the organization to improve understanding and capability maturity?
    - As challenges increase in complexity and scale, industry cooperation and information sharing about threats will become a valuable tool in the CISO's kit.

2 Heidrick & Struggles, "2022 Global Chief Information Security Officer Cisco Survey", 2022 https://www.heidrick.com/en/insights/compensation-trends/2022-global-chief-information-security-officer-ciso-survey

* Do you or a partner in your team have relationships with public-sector stakeholders such as law enforcement agencies (e.g., INTERPOL, EUROPOL, etc.), regulatory agencies' cybersecurity divisions, Computer Security Incident Response Teams (CSIRTs), etc.?

    ° Similar to cooperation with private industry partners, cooperation before an attack happens is becoming a pillar of sound security practices. See Principle 6 for more reasons to engage in cooperative relationships with these agencies.

* How often do you chat with CISO peers in your network about the challenges they are facing? What kind of peer exchange groups do you participate in that touch on risks facing our industry?

    ° Cyber capability can definitely be a competitive differentiator for companies in cyber product markets, but when it comes to dealing with common adversaries across any industry, it is important that the CISO and their team established very strong, non-competitive relationships with peer companies for threat intelligence information sharing for collective defence. These relationships are essential for both program and cultural maturity at all levels of the cybersecurity team, and work toward cooperative security.

DEEPEN THE RELATIONSHIP: MAKE THE CISO A STRATEGIC PARTNER

Like with all strategic partnerships, the relationship with the CISO needs to address the three "Cs": communication, collaboration, and coordination. These Cs enable the context for establishing independent roles but with shared benefits to the organization for managing contributions to stated strategic outcomes and risks. Start with a discovery session to gain a deeper understanding of what the risks are and align those to the board's strategic outcomes—this is where we can identify the partnership opportunity.

As noted earlier, one of the ways to engage strategically on information security topics is to focus on maturity and not just capability. CISOs tend talk about capabilities, so getting them to talk about the overall information security program forces the conversion away from technology and more toward people, process, and purpose. Ultimately, the tools available will not make your program mature. Rather, it's the people and the processes, and how effectively we are in using those to address business risks and strategic outcomes, that lead to success.

* Where have we made the most progress on cybersecurity in the past 12 months, and to what factor(s) is that progress attributable? Where do our most significant gaps remain, and what is our plan to close those gaps? Are the gap closure plans getting appropriately resourced or are those falling below the line of budget affordability? With whom is the CISO partnering to affect needed change throughout the organization? Is their relationship network up to the task?

* What is our cybersecurity workforce strategy? Do we have a strategy to recruit, retain, develop, rotate, and grow our personnel? With a decades-long war on cyber talent, mature programs are the ones that focus on talent and creating a culture where that talent can thrive and not just survive. When the people are happy, they bring their whole selves to work and that energy and commitment can really drive maturity around the mission.

The effectiveness of the program is the key metric. Once an organization has a well-educated and motivated workforce, it can turn attention to process maturity. An organization can be very good at what they do, but may not be very efficient or consistent in how they do it. Here is an area to focus on process performance with the CISO and their team to align with board objectives on performance and strengthen the cybersecurity program by aligning it with board performance objectives. In addition to implementing more automation to free up personnel to work on harder human-powered activities, one area to focus on in this category is analysing where we have "escapes" in the cybersecurity program—weaknesses in the program where effectiveness has eroded. Where are those exceptions that are driving the most risk? CISOs live these issues every day and have a strong interest in engaging with the board to help determine where the lines should be drawn in the sand for shared accountability and/or risk acceptance with the other corporate functions and lines of business.

* What organizations or locations have been exempted from one or more cybersecurity controls for business reasons?

    * For example, directors may hear CISOs mention topics such as critical applications only being patched during quarterly maintenance windows, research organizations bypassing Internet filtering, or factory systems not being scanned. While directors may not be familiar with the technical reasons behind why these are poor practices, they should understand that such exceptions to policy and controls increase the overall risk to the enterprise. Regardless of whether such exceptions are valid, management and the board need to be aware of the scope of the risk.

Lastly, engage with the CISO as an expert not just in the information security technologies arena, but also in emerging trends that could influence the competitive marketplace. Is there potential leverage for what we do internally to aid our external pursuits? Are there key external partners that can help us be successful? These types of conversations lead to a more strategic dialog with the CISO on how they can partner with the board to achieve these shared outcomes/objectives.

Tool I

ENHANCING CYBERSECURITY OVERSIGHT DISCLOSURES: 10 QUESTIONS FOR BOARDS

10 QUESTIONS FOR BOARDS

Note: This tool was adapted from How Cyber Governance and Disclosures are Closing the Gap, *a publication released by EY's Center for Board Matters, September 2022.*

This tool provides questions for directors to consider in preparing proxy statement or other disclosures related to the board's oversight of cybersecurity. It includes proxy statement disclosure data from US large-cap companies between 2018 and 2022, which boards can use for benchmarking purposes.

Cybersecurity remains front and centre on corporate agendas, as risks and regulatory requirements both continue to proliferate. In global surveys of CEOs and business leaders, cyber incidents are consistently named as the number one threat to business, edging out pandemic-related health risks, supply chain disruptions, and even macroeconomic volatility[1].

Investors and other stakeholders are paying attention, seeking more information on how boards and company leaders are overseeing and managing cyber risks. BlackRock, the world's largest asset manager, has stated, "[We believe] that data security is a material issue for more and more companies and regularly [engage] boards and management teams regarding the oversight and management of data privacy and security, crisis preparedness and response as well as related company disclosures[2]."In 2021, Institutional Shareholder Services (ISS) added 11 factors concerning oversight and management of information-security risk to its Governance QualityScore rating methodology[3].

EY's Center for Board Matters has tracked large-cap companies' proxy statement disclosures related to cybersecurity oversight since 2018. We have seen steady and significant increases in disclosures in several key areas, including:

* **Director skills and expertise:** disclosed by 61 percent of Fortune 100 companies in 2022, up from 35 percent in 2018;

* **Frequency of management reporting to the board:** disclosed by 68 percent in 2022, compared to 36 percent in 2018; and

* **Identification of a "point person" reporting to the board,** such as a chief information security officer: disclosed by 49 percent in 2022, up from 23 percent in 2018.

These increases in voluntary disclosures indicate companies are responding to investor and stakeholder interest in how their boards are overseeing areas that are vital to the firm's business strategy and risk profile.

Directors can use the ten questions below to help inform boardroom discussions about opportunities to enhance cybersecurity-related communications with investors and other stakeholders:

1. Do we understand the priorities of our company's major investors and other key stakeholders (suppliers, customers, employees, regulators, etc.) as they relate to cybersecurity, data privacy, and other key technology risk and strategy issues?

2. What feedback has senior management and/or investor relations received from our major investors? What questions are our top shareholders asking about how the company approaches information security and data privacy?

3. How is the company using disclosures to effectively communicate the rigor of our cybersecurity risk management program, and related board oversight activities, to investors and other stakeholders? What changes would be required in order to comply with relevant pending regulatory requirements, such as those of the EU's Cybersecurity Policy, and those of our other markets?

1 Allianz Risk Barometer 2022 (Allianz Global Corporate and Specialty SE, 2022); and Tim Human, "CEOs name cyber-risk as top threat in 2022, survey finds", Corporate Secretary, Feb. 2, 2022.

2 BlackRock Investment Stewardship Commentary, "Our approach to data privacy and security", (BlackRock Inc., 2022).

3 How cyber governance and disclosures are closing the gaps in 2022 (EY Center for Board Matters, 2022), p.8. https://www.ey.com/en_us/board-matters/how-cyber-governance-and-disclosures-are-closing-the-gaps-in-2022

4. Is cybersecurity mentioned in the risk oversight section of the proxy statement?

5. Do we describe which board committee or committees have responsibility for oversight of cybersecurity matters? Do we describe how the full board is involved in cybersecurity oversight, in addition to the activities of key committees?

6. Is cybersecurity included in our board skills matrix, or other description of skills resident on the board? Do we identify one or more directors as having cybersecurity expertise, and the criteria by which the board defines such expertise? How does professional cybersecurity experience, credentials, or other knowledge appear in directors' biographies? Do we disclose any education board members receive on cybersecurity topics, such as briefings from external advisors, law enforcement, or other third-party experts?

7. Do we describe how the board and/or key committees receive information from management about cybersecurity matters? Do we describe how the board and/or key committees consider cybersecurity matters as part of their deliberations on strategy, financial oversight, and enterprise risk management?

8. How does the relative prominence and/or specificity of the cybersecurity risk factors in our quarterly and annual reports compare with those in our current enterprise risk assessments?

9. How do we describe cybersecurity risk management activities, including:

    a. Policies and procedures

    b. Response planning, disaster recovery, or business continuity

    c. Simulations and tabletop exercises related to cyberattacks or breaches

    d. Education and training efforts

    e. Information-sharing with industry peers, law enforcement, etc.

    f. Use of an external independent advisor to support management and/or attest to cybersecurity assessment findings

10. How do our disclosures on board cybersecurity oversight compare to those of our competitors and industry peers?

Tool J

SECURING CLOUD SERVICES

- OBJECTIVE OF THE TOOL
- QUESTIONS BOARDS SHOULD ASK MANAGEMENT ABOUT THEIR CLOUD SECURITY STRATEGY AND CONTROLS

TOOL J

OBJECTIVE OF THE TOOL

Adoption of cloud computing services (or "the Cloud") continues to expand rapidly across industry. As companies migrate legacy capabilities and services to these new environments, they must develop new programs and capabilities to manage emerging cloud-centric risk patterns. This tool provides a high-level overview of the risks and set of questions to help board members evaluate management's approach to securing their new cloud services.

Understanding the full spectrum of cloud services is challenging as they come in many shapes and sizes. Cloud services can be a single virtual whiteboard application that allows remote workers to collaborate, a fully managed enterprise resource planning (ERP) platform, or a massive-scale hosting environment that replaces an organization's data centres. Whatever the application, what makes the cloud different is it puts a tremendous amount of power in the hands of each engineer or developer, allowing them to "point, click, and configure" individual cloud services to meet their business need. Unfortunately, this flexibility also creates risks where a single change or misconfiguration can inadvertently create a weakness that exposes the cloud services, the processes they enable, or the data they manage to risk.

Common patterns of cloud risks or threats include:

* **Misconfigured resources:** Inadvertent configurations can lead to access by unauthorized third parties; consume expensive processing resources, causing unplanned costs; or add unapproved applications to the company's cloud environment creating license risks.

* **Data leak or breach:** Failure to encrypt, secure, or properly manage cloud-based data storage or processing resources can expose sensitive data and trigger data breach notifications.

* **Malware infections:** Malicious software installed on unprotected cloud resources can spread "upstream" into the organization's data centres due to connectivity between the cloud and data environments physically located within an organization's premises.

* **Insufficient identity and access management controls:** Gaps in managing user identities and confidential information across services can expose corporate assets that are lacking appropriate authentication and access management controls.

The questions below are designed to help directors gain an understanding of the organization's cloud computing strategy and the programs, controls, capabilities, and resources that the organization and its management have employed to mitigate the risks associated with the strategy.

TOOL J

QUESTIONS BOARDS SHOULD ASK MANAGEMENT ABOUT THEIR CLOUD SECURITY STRATEGY AND CONTROLS

1. Are we adopting cloud-first strategy (i.e., all new assets in the cloud) or hybrid strategy (where we have some assets in cloud and some in traditional data centres)? Additional follow-ups:

    i. What percentage of our total assets are based in the public cloud today versus our existing data centres (e.g., 50—50%, 70—30%, 90—10%?)? What is our forecast over the next three years?

    ii. What percentage of our revenue generating assets are hosted in public cloud environments today and what is our forecast over the next three years?

2. What were the major factors that drove the decision to migrate and expand adoption of cloud services?

    i. Elasticity. Was the ability to rapidly scale to support increasing customer demands, integrate new acquisitions, or expand to new geographies critical to the decision?

    ii. New Innovations. Was there the desire to take advantage of the cloud service providers' investments in emerging capabilities and services?

    iii. Compliance and Security. Did the significant investment in security controls and existing compliance with prevailing standards and frameworks (e.g., ISO, NIST) that cloud providers are held to play a role in the decision?

    iv. Reduce Cost by Divesting Our Expensive Data Centres. Were we able to increase capacity requirement with this choice? Did it allow the reduction of constant technology changes (hardware and software refreshes), data centre contract renewals, and other challenges?

3. What types of business processes are we using cloud-based resources to create or refine?Is our plan to:

    i. Use limited Software as a Service (SaaS) for employee productivity and back-office processing?

    ii. Will we be using cloud services to store, process, and manage our sensitive confidential information?

    iii. Will we be hosting, processing, and controlling our customers' sensitive information in cloud services?

    iv. Will we be fully exiting our current data centres and shifting all hosting services to public cloud service provider environments?

4. Do we understand our SaaS ecosystem, and how and where each cloud service provider is storing our sensitive data for:

    i. Corporate Systems (e.g., ERP, HR, Payroll)

    ii. Productivity Tools (e.g., MS Office, Google Suite)

    iii. Sales & Marketing (e.g., pricing, orders, etc.)

    iv. Customer master data (e.g. customer lists)

    v. Products and Applications (hosted environments)

5. What's is the organization's strategy for partnering with major cloud service providers (CSPs)? Items to consider are listed below:

    i. How are we avoiding CSP concentration risk? What percentage of our services are deployed in AWS, Azure, Google Cloud Platform (GCP), and/or other cloud environments?

    ii. Are all our cloud services in one cloud environment that is hosted in one geographic location or are they dispersed geographically? How is the organization avoiding the risk of data centres being concentrated in one locality?

    iii. What security certifications and accreditations do our CSPs maintain?

    iv. Do we have a decision tree that would suggest best CSP provider for our organization?

6. What level of support have we contracted with our core cloud service provider and what does that level provide?

    i. Does that support level meet the demands of our risk appetite?

    ii. Do we have well defined SLAs to meet optimum level of service availability?

7. Do we have clear roles and responsibilities defined between the organization, the CSPs, and third-party vendors? Are contracts for services aligned to a shared security responsibility model?

8. How is the organization managing top cloud security threats and risks including, but not limited to, data exposure? Some tactics that boards can ask about include:

    i. Data protection and compliance programs driven by employees

    ii. Embedding industry aligned cloud security framework-based requirements in the contracts

    iii. Managing and tracking cloud spending via cloud cost management tools

    iv. Building strategic partnerships for faster access to capabilities

9. How are we governing CSPs? Tactics for boards to listen for when management discusses CSP governance include audits/review, quarterly business reviews, and service reviews by contract service level agreements.

10. Does our organization have the right expertise in cloud to support the business and cloud strategy? Directors and management should scan the talent in the organization to see if it includes leaders with deep experience in cloud, programs to incubate and maintain internal talent, online subscription-based training and certification-based programs, and attendance at vendor conferences with training programs.

11. How does our cloud strategy support our customers' needs while also enabling our organization's workforce to better serve themselves and others? Some benefits of cloud computing to the workforce and customers include the following:

    i. Brings organization closer to users/customers

    ii. Supports data localization laws and regulations

    iii. Enables hybrid working in secure way

    iv. Breaks the barrier of cost around training IT and security staff on management of on-premises data servers

12. How are we measuring our cloud spend and savings generated? Consider asking management if the following standards are being met during measurement:

    i. Processes established to monitor trends and modify license agreement

    ii. Enforcing tagging standards across the organization

    iii. Persistent tracking with cloud cost management tool that is also shared with users to monitor their own cloud consumption and spend

Tool K

SUPPORTING NATIONAL SECURITY AND FIVE TRIANGULATING QUESTIONS FOR BOARD MEMBERS TO ASK THEIR CISOS

- OBJECTIVE OF THE TOOL
- NATIONAL SECURITY IS A SHARED RESPONSIBILITY
- TECHNOLOGY PROVIERS HAVE A SPECIAL IMPACT ON NATIONAL SECURITY
- TRIANGULATING QUESTIONS

TOOL K

OBJECTIVE OF THE TOOL

Cybersecurity is a shared national responsibility. This tool will help boards understand their role in supporting national security. In addition, the tool includes five questions to help spark conversations to generate fresh insights into the effectiveness of security programs.

NATIONAL SECURITY IS A SHARED RESPONSIBILITY

Now more than ever cyber risks extend beyond the boundaries of an enterprise to affect other companies and the critical infrastructure and services that underpin major functions of society. The government your country needs your help in collaboratively addressing cyber risks with national security implications. Benefits for your company or organization for addressing national security risks include:

* Mitigation against significant financial loss from targeting by sophisticated threats;
* Reduced regulatory scrutiny and liability exposure;
* Improved resilience against operational or functional disruption;
* Focus of your company or organization's cybersecurity program on the most significant national risks; and
* Continued competitive advantage in a global market.

TECHNOLOGY PROVIDERS HAVE A SPECIAL IMPACT ON NATIONAL SECURITY

Because cyber risks of technology providers can create risk for their customers, technology providers can have an exponential impact on national security and the public good. Directors at companies and organizations that develop and maintain technologies used by other parties should ask your company managers to:

* **Prioritize multi-factor authentication (MFA) by default.** For customers using your products, MFA should be mandatory for administrators as a default setting and all users should be firmly nudged toward using MFA.
* **Write secure software.** Your company should consider writing new software projects in memory-safe language, publish Software Bills of Materials, and publish vulnerability advisories in machine-readable format.
* **Prioritize secure default configurations.** Your company should consider offering security features at no extra charge, especially single-sign-on and multi-factor authentication.

TRIANGULATING QUESTIONS

Executive leadership and boards need more than one way to evaluate their security programs. These programs have many moving parts and it's often hard to know how they will stand up to dedicated, human adversaries who often work in long-term campaigns. The following questions can help spark conversations to generate fresh insights into the effectiveness of security programs.

These questions are not intended to be gotcha questions and board members should approach these questions in the spirit of helping CISOs who need support and guidance. Should any of these questions reveal gaps in the security program, the overall team can help understand why and plot a new path forward.

Question 1

Regarding our email server

a. What percentage of users do not need to use MFA when logging in?

b. How many system administrators are there?

c. How many administrators do not need to use MFA when logging in?

d. Which executives do not need to use MFA to log in?

Why is it important?

A large percentage of compromises involve credential phishing at some point in the attack chain. Yet many organizations have not yet deployed MFA to 100 percent of staff and 100 percent of system administrators, even for critical systems like email. This disconnect often has roots ranging from employee or executive resistance to lack of MFA support in legacy systems, or in prioritization.

You can iterate on that question for other systems, like file storage or single sign-on (SSO) systems.

Helpful answer:

Given today's threat landscape, enterprises should have already made MFA the default for all staff and privileged users, especially system administrators. At a minimum the security team should be able to provide the percentages and a list of exempted users without much effort.

The ideal answer is that all systems are behind an SSO portal, and that portal requires MFA for all users.

Answers that demand more prodding:

The list of users who are exempted from MFA for email systems will generally be short and temporary, like for users during onboarding or while they are transitioning to a new phone. But often there are user accounts that are permanently exempted, and the team should evaluate the resulting risk.

Question 2

Regarding our identity/SSO system

a. What are our greatest weaknesses?

b. What systems are not yet protected by being behind our identity system?

Why is it important?

It's a standard practice to centralize identity and access management (IAM) into a single or federated identity system such as Active Directory or any one of several cloud-based alternatives. A compromise of this system would have catastrophic implications for all other systems within an organization, like email, file storage, HR systems, financial systems, and so on.

The old security saying is "Put all your eggs in one basket, and *really watch that basket!*" The question here is to what degree the organization is watching that basket.

Helpful answer

Because IAM systems are so critical, the security team should be able to talk about a range of topics starting with configuration management. Many products, including IAM products, are delivered to the customer with surprisingly unsafe defaults. The team may talk about that fact, and possibly their experience with the vendor's hardening guide.

Security staff may talk about the challenge of working with HR to ensure staff are properly offboarded when they leave and discuss minor incidents or near misses when that didn't happen. They may talk about how they monitor for unauthorized logins and also about the limits of those approaches.

The team will generally have a punch list of products that are not behind the IAM system and a roadmap for migrating them to that central service.

Answers that demand more prodding

IAM systems are hard to build and maintain securely and require good partnerships with teams like HR (for employee onboarding/offboarding) and procurement (which often handles vendor accounts—another gap worthy of discussion). If the CISO hasn't personally seen IAM processes and technologies fail, they may need to do some additional research and outreach to their peers.

Question 3

Describe our company's "shadow IT" situation in terms of data, services, culture, origins, and the resulting risk. What is being used without explicit authorization?

Why is it important?

Organizations will often have users and groups whose workflow includes the use of products not sanctioned by IT and security teams, often free online services. While the staff are trying their best to get their jobs done, shadow IT services can cause data leakage and create avenues for compromise.

Given how common it is for an organization to have some form of shadow IT, it's important for the CISO to factor it into the organization's overall risk analysis. Measuring the prevalence of shadow IT in the organization can be challenging since these tools and workflows are by definition off the books.

Helpful answer

A productive conversation would include a discussion about where pockets of shadow IT live, which staff/teams are using these tools, and how staff are utilizing these tools to compensate for or complement sanctioned IT products and services. Are they unaware of official tools, or dissatisfied with them? Or perhaps there are cultural and team reasons to use non-standard tools.

Answers that demand more prodding

It would be surprising for the CISO to not have stories about shadow IT, perhaps signalling that they need to reach out to various groups to solicit input on the approved toolsets and to be open to people explaining why they are building their own.

Question 4

If the board and management could eliminate (or at least take ownership for) employee pushback, what two changes (across people, processes, technologies) would you make to dramatically improve our security posture? How would those changes raise the cost of attack for possible adversaries?

Why is it important?

There is a general tendency for security teams to try to secure existing products and workflows, usually by adding security tools. The goal is to secure the organization without disrupting users and workflows. While this approach can work, it has its limits. To achieve higher levels of security, organizations may need to consider radically refactoring their workflows and tools. To use a car analogy, it may not be possible to add airbags, collapsible steering columns, and crumple zones to a car from 1960. A redesign is what gives you those safety measures.

The board can generate conversations and interest in ideas that might encounter employee resistance but could dramatically improve the security posture. A security team might not be empowered to work against company culture, but a CEO might be able to manage it.

One minor example: FIDO security keys can eliminate credential phishing (even MFA-bypass attacks) but may cost money and require employee training. It may be challenging for the CISO to drive the cultural change alone and they may not have raised the issue. Discussing these big-bet ideas should be a natural part of board conversations.

If you were building the company or organization from scratch, would you build it the way it currently exists? Would you secure it in the same way? The answer is probably no. Discussing the delta between those two models can be illuminating.

Helpful answer

Some CISOs have a slide deck with their big bet ideas already documented. Most should be able to create such a deck in conjunction with other teams.

Answers that demand more prodding

Company culture and technical debt limit how much an organization can refactor at any given point in time. Yet security and partners in CIO and CTO organizations generally understand those limits. Dig deeper if the answers you get indicate comfort with the status quo and current trajectory for improving the organization's security posture.

Question 5

Knowing everything you know about our security posture and the broad spectrum of attackers in play, how would you break in to steal data from the company?

If you had a budget of one million dollars to hire a crew with specific talents, who would you hire and for what tasks?

Why is it important?

We frequently hear the phrase "think like a hacker," but even security professionals can find it hard to constantly adopt that mindset. How might someone chain together seemingly unrelated and minor vulnerabilities into a major intrusion?

Helpful answer

If the CISO can refer to previous information they've presented and connect the dots, you have a successful answer.

Possible answers

"I'd get someone to bribe a call-centre employee to install cheap, commodity malware on their system. As I mentioned before, our call-centre network is connected to our production network, so a compromise of any one system there gives an attacker access to our customer data."

"I'd hire someone to compromise that small company we just acquired. We haven't imposed our security controls on them for political reasons. Their network is separate, but they have privileged access in our development environment. Not only might we not be able to prevent the attack, but we also probably couldn't detect it."

Answers that demand more prodding

Every security professional should have several ideas on how such an attack might happen. If the CISO doesn't have any ideas, they may be in "maker" mode and will need help getting into "breaker" mode. Even conducting a tabletop exercise can generate creativity and deeper insights.

Still, the attacks should be relatively simple to execute and not spy fantasies. When they are compromised, most organizations are not attacked by intelligence agencies spending millions of dollars and dozens of team members. Far too many are compromised because they ran unpatched software, didn't segment their networks, lacked MFA, and allowed users to run arbitrary software on their laptops.

Tool L

TOOL FOR THE BOARD OF DIRECTORS TO DECIDE GENERAL USE OF ARTIFICIAL INTELLIGENCE

- OBJECTIVE OF THE TOOL
- DEFINING ARTIFICIAL INTELLIGENCE, MACHINE LEARNING, GENERATIVE AI AND LLMS
- GENERAL QUESTIONS FOR THE BOARD TO CONSIDER IN OVERALL USE OF AI/ML
- QUESTIONS FOR THE BOARD OF DIRECTORS TO DECIDE GENERAL USE OF AI FOR CYBERSECURITY PURPOSES

OBJECTIVE OF THE TOOL[1]

Much like the Internet itself artificial intelligence (AI) and machine learning (ML) are already becoming ubiquitous tools in many organizations. In 2023, private investment in AI totalled around $95.99 billion—a slight decline from 2022[2] — while private investment for generative AI alone surged to $25.2 billion[3]. Also, as with the Internet, the use of AI and ML tools can provide dramatically enhanced business opportunities in terms of efficiency, innovation, and customer service. At the same time, the use of AI and ML can create vast new risks in terms of cybersecurity. The US National Security Commission on Artificial Intelligence found that "AI applications are transforming existing threats, creating new classes of threats, and further emboldening state and non-state actors to exploit vulnerabilities in our open society[4]."

Just as with the flip side of many other risks, certain applications of AI and ML tools can be used to enhance an organization's cybersecurity and lessen its risks. It is critical that the board work with management to understand the risk-reward balance of the specific uses of AI/ML their organization should embrace. This tool consists of two lists of questions to help guide the board's oversight of these advanced digital techniques. The first list is for the board's overall consideration of using various AI/ML techniques. The second list focuses on the specific issues in the use of AI for cybersecurity.

Defining Artificial Intelligence, Machine Learning, Generative AI and LLMs

***Artificial Intelligence (AI)**, a term coined by emeritus Stanford Professor John McCarthy in 1955, was defined by him as "the science and engineering of making intelligent machines". Much research has humans program machines to behave in a clever way, like playing chess, but, today, we emphasize machines that can learn, at least somewhat like human beings do.*

***Machine Learning (ML)** is the part of AI studying how computer agents can improve their perception, knowledge, thinking, or actions based on experience or data. For this, ML draws from computer science, statistics, psychology, neuroscience, economics and control theory.*

Companies need to weigh opportunities and threats of getting involved with the newest GenAI solutions, also popularised by current vendors like Microsoft or Google. Board members need to be cognizant of both sides.

1 The following questions are designed primarily based on the "A.I. and Risk Management: Innovating with confidence report" by Deloitte (https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/deloitte-gx-ai-and-risk-man agement.pdf) and "Attacking Artificial Intelligence: A.I.'s Security Vulnerability and What Policymakers Can Do About It" by Harvard Kennedy School Belfer Center for Science and International Affairs (https://www.belfercenter.org/publication/AttackingAI). Sun, Simon. 2022. "Artificial Intelligence and Cybersecurity Risks." Indiana University.

2 Stanford Institute for Human-Centered Artificial Intelligence. 2024. "Artificial Intelligence Index Report 2024" Stanford University, p. 243 (https://aiindex.stanford.edu/wp-content/uploads/2024/05/HAI_AI-Index-Report-2024.pdf).

3 Stanford Institute for Human-Centered Artificial Intelligence. 2024. "Artificial Intelligence Index Report 2024" Stanford University, p. 216 (https://aiindex.stanford.edu/wp-content/uploads/2024/05/HAI_AI-Index-Report-2024.pdf)

4 DAIMLAS Artificial Intelligence Ecosystem Builders, [@DAIMLAS]. (2022, June 10). AI applications are transforming existing threats creating new classes of threats and further emboldening state and non-state actors to exploit vulnerabilities in our open society [Tweet]. Twitter. https://twitter.com/daimlas/status/1535389680195207168

OPPORTUNITIES	RISKS
* Using GenAI tools to increase productivity of employees, especially those whose part of job is creating documents or content * Improving quality of content outputs, including customer-facing content * Improving quality of documents, enriching their thoroughness * Improved analytics and reasoning based on available company data * Reduction of workforce cost for mundane and manual jobs or customer service jobs (through high-quality chat-bots)	* Many AI tools require provision of data inputs. Employees might upload company data without understanding the risk profile of the service. * Relying on information and sources that are not 100% reliable as AI has a goal to give any answer even when not having the truth (hallucinations) * Misuse of content resulting in lawsuits regarding intellectual property rights * Usage of personal data in ways not in line with GDPR policies to generate personalized content for customers or employees.

At the moment of publishing of this document the current legal document regarding AI in the EU is the AI Act https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai. The document lays out the key considerations regarding AI risk.

GENERAL QUESTIONS FOR BOARD TO CONSIDER IN OVERALL USE OF AI/ML

1. What is the goal for the company or organization thinking of employing AI/ML?
2. What is the plan to build or deploy this AI or ML application responsibly?
3. What type of system is the company using: process automation, cognitive insight, cognitive engagement, or some other type? Does our board and management understand how this system works?
4. What are the economic benefits of the chosen system?
5. What are the estimated costs of not implementing such a system?
6. Are there any potential alternatives to the AI or ML systems in question?
7. How easy will it be for an adversary to execute an attack on the system based on the technical characteristics?
8. What is the organization's strategy to validate dataset collection practices?
9. How will the company prevent inaccuracies that may exist in the dataset?
10. What will be the damage incurred from an attack on the system in terms of the likelihood and the ramifications of the attack?
11. How frequently will the company review and update its data policies?
12. What is the organization's response plan for cyberattacks involving these systems?
13. What is the company's plan to audit the AI system?
14. Should the company create a new team to audit the AI or ML system?
15. Should the company build an educational program for its staff to learn about the use and risks of AI and ML in general?

TOOL L

QUESTIONS FOR BOARD OF DIRECTORS TO DECIDE USE AI FOR CYBERSECURITY PURPOSE[5]

1. What is the company's overall roadmap to implementing AI and/or ML in cybersecurity?
2. What are the cybersecurity goals that the organization is trying to achieve by implementing this AI or ML solution?
3. How will the system toughen the companies' security stance? How will success be measured?
4. What is the estimated harm that the company will face without the system?
5. What are the new cybersecurity vulnerabilities that the company will face employing the system?
6. What type of cyberattack is the system designed to detect, predict, and respond to?
7. Is the system prepared to detect and weather a ransomware attack?
8. How would implementing such a system affect the organization's cybersecurity team? What are the benefits and risks associated with the tool's use by the team?
9. Should the company expand or update the current cybersecurity team?
10. How much would it cost for the company to create a new cybersecurity team?
11. Are there any positions that the company doesn't need any more due to employing the AI or ML cybersecurity system?
12. Should the company create a sub-team to monitor the outcomes and findings of the new system?
13. Will implementing such a system affect the company's cyber insurance enrolment?
14. Are there any potential legal consequences of not implementing AI/ML in a cybersecurity system?

5 The previous tool questions should apply in this section as well as both are referring to the use of AI systems.

MEMBERS OF THE WORKING GROUP

Key writers:

Larry Clinton
President/CEO
Internet Security Alliance (ISA)

Parker Phillips
Manager for Policy and Government Affairs
ISA

Advisors:

Tomi Dahlberg
Ph.D (Econ), Board professional, ISS Professor at Turku School of Economics (ret.), Senior Advisor
Directors' Institute Finland (DIF)

Tanja Dreilich
M.Econ, MBA CFO, Supervisory Board Member, Financial and ESG Expert Former CEO
NEMTF

Kasia Kazior
AI Digital Transformation Executive, Supervisory Board Member
Benefit Systems SA (WSE: BFT)

Beatriz Lara Bartolome
NED at UniCredit S. p. A.
Chair of Chapter Zero Spain

Uroš Žust
Partner IT Assurance & Advisory
Forvis Mazars

Béatrice Richez-Baum
Director General
ecoDa

TOOL L

ADDITIONAL CONTRIBUTORS

JR Williamson
Sr, Leidos

Tracie Grella
AIG

Jon Brickey
Mastercard

Deneen DeFiore
United Airlines

Dimitrios Stratakis
BNY Mellon

Kris Lovejoy
Kyndryl

Kelly Bissell
Microsoft Services Group

Brad Maiorino
RTX

Tim Held
US Bank

Ted Webster
Centene

Patrick Hynes
Ernst and Young

Niall Brennan
SAP

Greg Touhill
Carnegie Mellon University

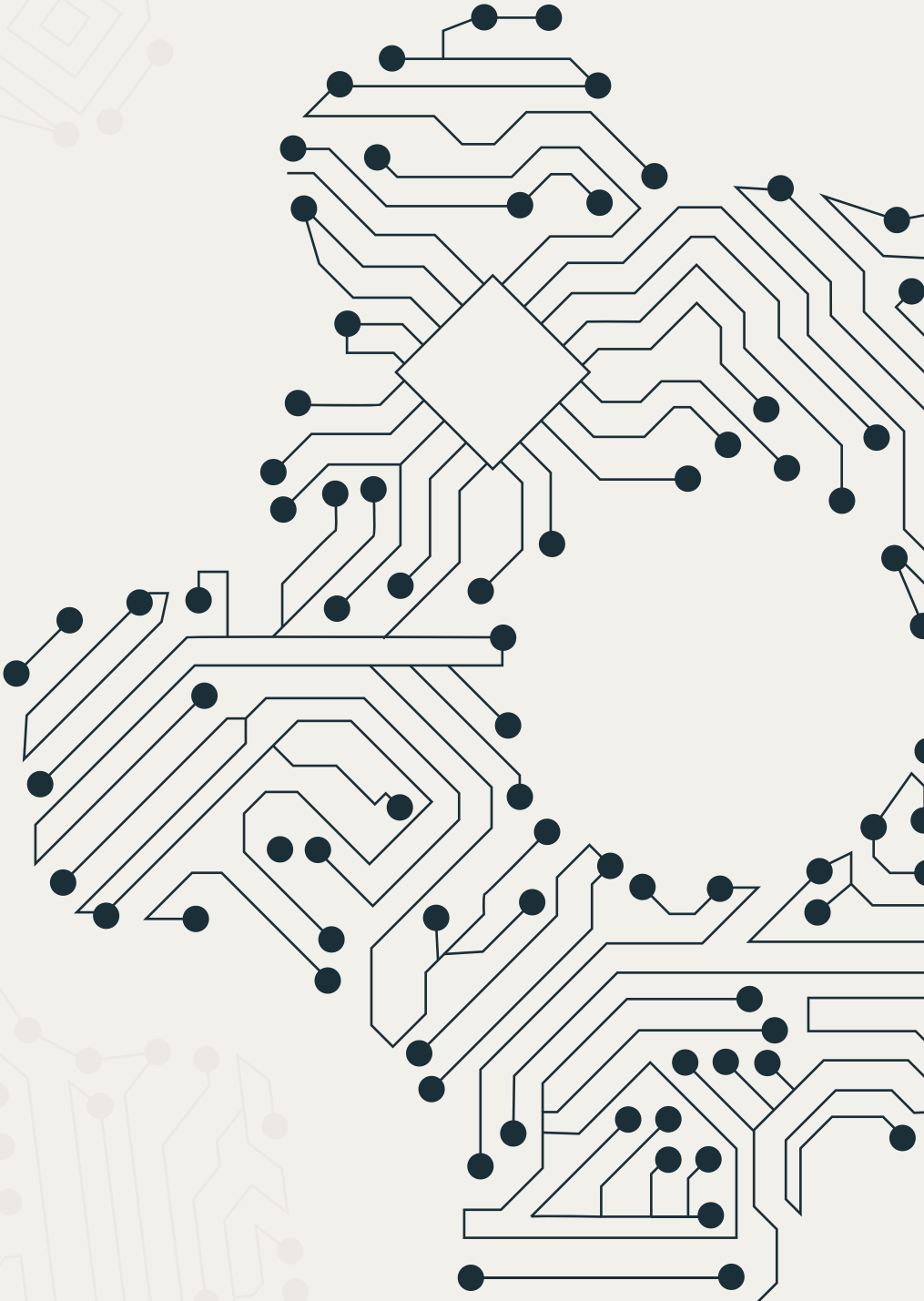
Franck Journoud
National Association of Manufacturers

Richard Rocca
Bunge Limited

Ryan Boulais
AES Corp

Patrick Reidy
GE Aerospace

Michael Higgins
L3 Harris



ecoDa
Avenue des Arts 41
1040 Brussels
Belgium
T: 32 (0) 2231 58 11
contact@ecoDa.eu