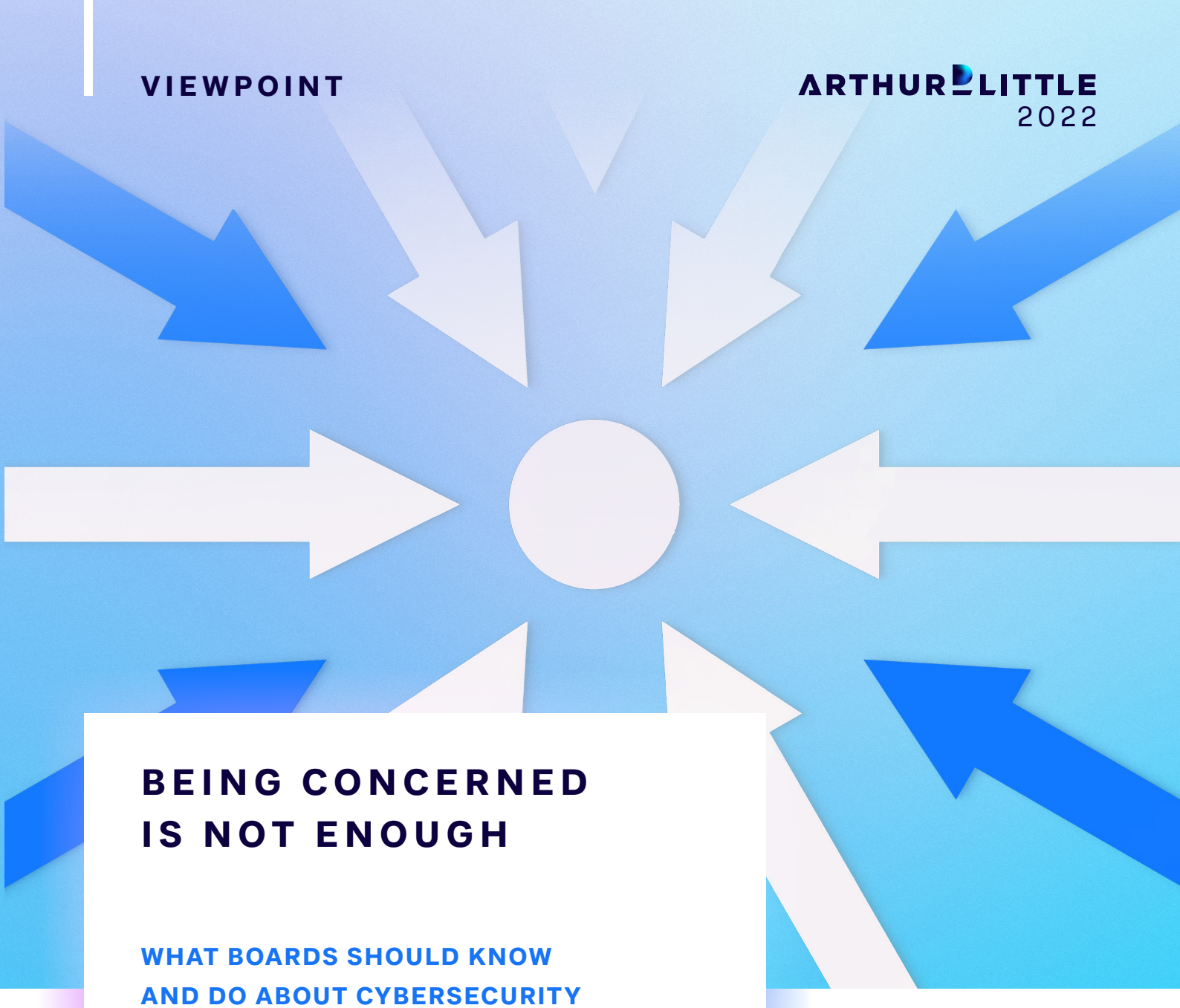
VIEWPOINT

ARTHUR D LITTLE
2022



BEING CONCERNED IS NOT ENOUGH

WHAT BOARDS SHOULD KNOW AND DO ABOUT CYBERSECURITY

Continuous growth and diversification in the cybercrime landscape, accelerated by the COVID-19 pandemic, have increased the relevance of well-performing IT/operational technology (OT) cybersecurity. But cybersecurity's complexity inhibits understanding and is thus often relegated to a mere part of the IT budget. Arthur D. Little's Cybersecurity Matrix enables targeted assessments, allowing organizations to pinpoint key issues and prioritize remediation actions accordingly. These readily understandable insights facilitate board discussions that are long overdue.

AUTHORS

Maximilian Scherr

Tom Teixeira

Dmytro Zaika

Michael Ludescher

CYBERSECURITY IS EVER-INCREASING IN RELEVANCE

Cybersecurity is a critical topic for both the private and public sectors. Since the first relatively harmless cyberattack in 1988, the cybercriminal space has evolved to become a major threat to the physical and nonphysical worlds alike. In response, governments and organizations must allocate the resources required to prevent cyberattacks against their information and operation systems. At the same time, companies are exposed to a rapidly changing threat landscape as well as a recent spike in cyberattacks due to the COVID-19 pandemic. Without a clear understanding of cybersecurity, organizations will find it nearly impossible to effectively protect against cyber threats.

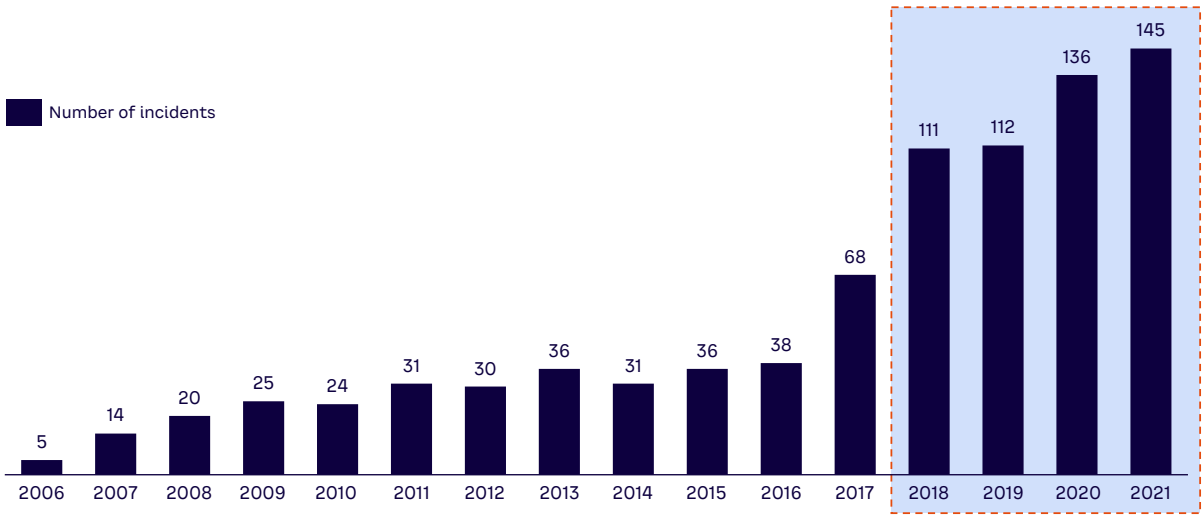
Between 2015 and 2020, the number of significant cyberattacks on key infrastructure establishments, or economic crimes that exceeded US $1 million in losses, more than tripled (see Figure 1). In 2021, total damages from cyberattacks exceeded $1 trillion worldwide, up more than 50% from 2018 levels. Meanwhile, the conflict between Russia and Ukraine has contributed its share of cyberattacks in 2022, leading to a massive surge globally.

The escalation in damages is unprecedented and puts cybersecurity well on its way to becoming the most serious business threat of the future. As a matter of course, this development did not escape the attention of insurance firms. Companies are facing rapidly increasing premiums, reflecting the surging demand for cyberinsurance and the higher risk exposure, putting additional pressure on already limited cybersecurity budgets. Therefore, executives should be aware not only of the increase in the number and severity of cyberattacks but, even more importantly, about the changing threat landscape.

Major cyberattacks transform threat landscape

The examples included in the sidebar describe some of the transformative cyber incidents against key points of global supply chains. They demonstrate the real-world impact and diversification of cyber threats and reveal the importance of management's increased attention on cybersecurity.

Figure 1. Number of cyber incidents with more than US $1 million in losses



Source: Arthur D. Little, CSIS

4 recent transformative cyber incidents

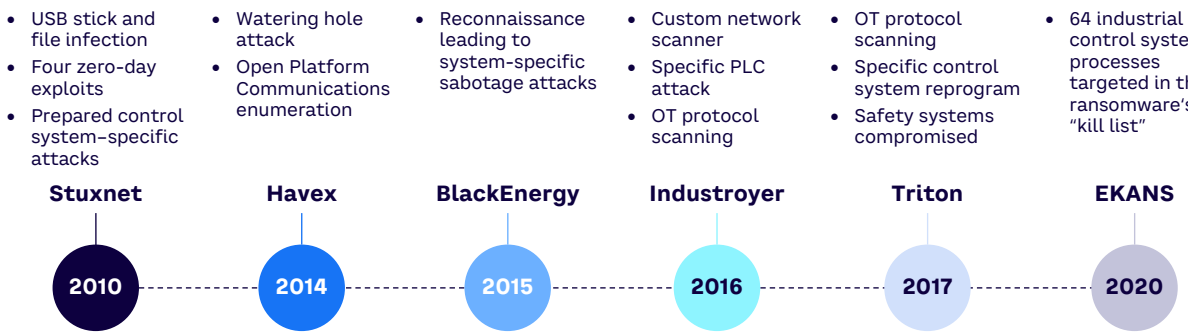
1. **First major cyber incident for operational technology.** In 2015, a criminal group hacked Ukraine's electrical grid system, leaving approximately 230,000 homes without electricity for up to six hours. The cyberattack marked the first major OT outage due to a cyber incident in history.
2. **Cyberattack with severe global impact.** In 2017, Maersk was subject to one of the most severe cyberattacks in recent history. Ransomware blocked internal systems, leaving the company unable to process customer orders. The shutdown of OT systems cost the company in excess of $300 million in damages.
3. **Cyber incident with potential impact on human health.** In February 2021, hackers gained access to the control terminal of a water treatment plant in the US state of Florida, then increased the amount of a toxic chemical in the water to dangerous levels. A plant operator noticed the increase and immediately corrected the chemical levels. Nonetheless, the attack exemplifies the vulnerability of key infrastructure with potential harm for human health.
4. **Cyberattack on critical infrastructure.** In June 2021, a hacking group launched a ransomware attack against Colonial Pipeline on the East Coast of the US and forced the shutdown of the pipeline as a precautionary measure. As a result of the shutdown, many gas stations had to limit service due to fears of gasoline shortages. This attack exemplifies the impact of cyber incidents on operators of essential services.

Cyberattacks on operational technology

The focus of cybersecurity has traditionally been on IT systems. However, in the last decade, cybercriminals have repeatedly targeted OT (see Figure 2). The growing number of attacks on OT demonstrates that cybersecurity is not just about protecting information but also about process safety. Cyber incidents increasingly bear operational and physical risks that can lead to significant business interruption.

The traditional belief that OT is separated from the outside world no longer holds true due to the advancing convergence of IT and OT systems. As part of the fourth industrial revolution, or Industry 4.0, the (Industrial) Internet of Things (IoT) is gaining a foothold in most organizations, leading to the deployment of more and more IT-like systems within OT environments to support key processes. While companies see the vast performance and efficiency gains associated with leveraging their operational data for advanced

Figure 2. Key cyberattacks on operational technology



Source: Arthur D. Little, Darktrace

analytics purposes, they often neglect the additional cybersecurity risks. In line with this, a 2021 study by Palo Alto Networks found that 96% of IT decision makers admit that their current IoT security approach shows upside potential, highlighting capabilities like threat protection, risk assessment, or asset management as their main pain points. Furthermore, the study found that 98% of all IoT device traffic is unencrypted and 57% of IoT devices are vulnerable to medium- or high-severity attacks.

Exposing a growing number of physical devices to the outside world not only increases the complexity of ensuring sufficient security standards but also broadens a company's attack surface (i.e., its sum of potential targets for a cyberattack). The very nature of IoT devices, being closely interconnected with each other, amplifies the risk of spreading, since a compromised device may contaminate an entire system.

The growing number of cyberattacks on OT means that operators of critical services (such as oil and gas suppliers or utility companies in their crucial role within global supply chains) must ensure awareness and effective protection against cyber threats all the way down to the shop floor.

Acceleration of cyberattacks due to COVID-19

According to a 2020 study conducted by ADL, top management executives confirmed that the COVID-19 pandemic required additional processes and security measures for 36% of companies. Moreover, 46% of companies have provided employee training and 43% have implemented additional awareness campaigns to ensure data and information security.

REMOTE WORKING, REPRESENTED A FUNDAMENTAL CHANGE IN THE CYBERSECURITY THREAT LANDSCAPE

The pandemic marked a shift in working patterns toward remote working, representing a fundamental change in the cybersecurity threat landscape. Workers moved from better-protected corporate networks to relatively unsafe and often wrongly configured home networks, presenting a critical vulnerability for corporate information. In particular, a rise in ransomware attacks conducted via VPNs used for remote working access (as in the case of Colonial Pipeline), poses a significant cyber threat. Criminals exploit these newfound security deficiencies to their advantage, accelerating the already growing threat of cyberattacks.

The work-from-home (WFH) culture that developed during the pandemic is not anticipated to end, with numerous studies estimating that 25%-30% of the global workforce will continue to WFH at least several days a week for the short and medium term, meaning this increased risk is likely to remain.

CORPORATE CHALLENGES WITH CYBERSECURITY

To address cybersecurity successfully, businesses must overcome three central challenges:

1. **Visibility.** The inherent complexity of cybersecurity has to be translated into understandable, action-oriented recommendations for top management.
2. **Resource allocation.** Companies must address the apparent mismatch between the economic damage of cyberattacks and their cybersecurity investments.
3. **Measurement.** Companies need sophisticated cybersecurity measurement systems to track progress and clearly communicate key issues to top management.

1. Visibility

The complexity of the cybersecurity topic inhibits key management attention and focused action. Often, C-level executives do not easily understand the technical information operational IT staff shares. To address this issue, many corporates adhere to international standards as a benchmark of good cybersecurity practice.

There are two commonly applied standards within IT and OT cybersecurity, respectively: ISO 27001 and IEC 62443. Both standards include multiple domains and secondary objectives with high levels of technical detail that make them difficult to interpret and communicate to key decision makers. Of course, international standards bodies are already addressing this challenge by gearing recent versions of their standards toward reduced complexity. In its 2022 update of the well-established ISO 27002, the International Organization for Standardization serves as a prime example, not only reacting to the changing threat scenarios but also discarding its 14 control domains in favor of four more comprehensive categories/themes as well as reducing the total number of controls by means of merging or minimizing redundancies. While such updates are undoubtedly a major stride toward the desired goal, the challenge of striking a balance between maintaining the required technical level of detail while achieving general comprehensiveness, especially for top-level management, remains a crucial one.

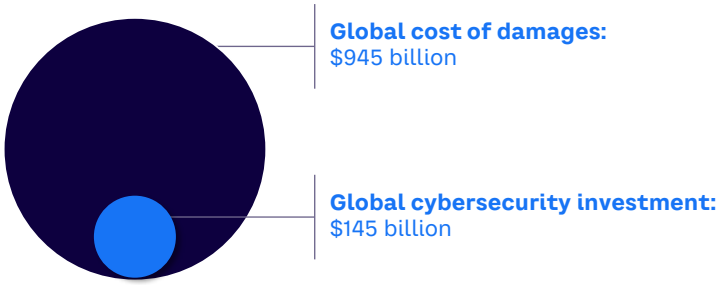
In addition to the challenges of communication, the standards' mode of assessment is targeted toward compliance rather than recommendations for improvements. ISO and IEC compliance is examined with a questionnaire type of assessment, whereas expert-type assessments are often missing.

Real expert-type assessments are geared toward a "show me, don't tell me," attitude and enable the assessment of cybersecurity performance in action. For example, an assessor may ask a firewall operator to access certain logs or show how security configurations have been implemented. Measuring compliance with ISO/IEC or similar standards is a minimum (but not sufficient) requirement that needs to be set before conducting an expert-type assessment.

2. Resource allocation

In 2020, the global costs of cybercrime exceeded $1 trillion, according to a McAfee report. The loss in damages from cyberattacks has reached an estimated $945 billion, while companies have invested only $145 billion in cybersecurity (see Figure 3).

Figure 3. Global cost of cybercrime relative to cybersecurity investment



Source: Arthur D. Little, McAfee

On an organizational level, the mismatch between potential damages and preventive investments looks similar. McAfee estimates the average cost of a data breach for American corporates is approximately $8.64 million, while an average organization spends only $2.6 million on cybersecurity. This clear gap leaves organizations vulnerable to growing cyber threats.

In an attempt to close the resource gap and to defend an organization effectively against cyberattacks, information security is becoming one of the top priorities within the IT budget. IT spending (including for cybersecurity) is often seen as a cost driver rather than an enabling factor for businesses. This means that during crises, companies tend to reduce their respective budget allocation.

Moreover, companies oftentimes prioritize cybersecurity spending only after a major incident. The potential reduction in cybersecurity investment is a worrying trend, particularly given the continuous increase in the number of cyber threats. This mismatch shows the need to focus financial resources on the most impactful measures, which requires a clear prioritization framework.

3. Measurement

It is impossible to guarantee full protection from cyber threats. However, certain indicators can highlight the increased risk to better prepare organizations. Still, holistic measurement of cybersecurity effectiveness is challenging.

Calculations of ROI indicators of a cybersecurity program are especially complex, as returns on cybersecurity can only be reflected as the opportunity cost of damages from a cyberattack or an estimated value of cyber risk documented by corporate risk and compliance. To address this challenge, ADL has compiled preventive and reactive measures, indicative of the preparation levels of organizations against cyberattacks. These include "lagging" KPIs like critical vulnerabilities and security incidents that point to cybersecurity issues that already exist in organizations. Alternatively, "leading" indicators include KPIs (e.g., threat intelligence, total risk exposure, and security awareness) that point at general preparedness (see Figure 4).

MEASUREMENT & ACTION PLAN

Digesting cybersecurity standards

Cybersecurity must be broken down into its components to enable targeted action. As mentioned earlier, there are several commonly applied standards within IT and OT cybersecurity, including ISO 27001, IEC 62443, and NIST (see Figure 5). These standards include multiple domains and secondary objectives with high levels of technical detail. Consequently, the standards are difficult to interpret and communicate to senior decision makers, making prioritized action planning with corresponding resource assignments challenging.

Figure 4. Examples of cybersecurity KPIs

LEADING INDICATORS

- **Cyber threat intelligence**
  (# of threats to an industry)
- **Cyber risk exposure**
  ($ value of documented risks)
- **Cybersecurity maturity level**
  (Score 0-5)
- **Security awareness**
  (Corporate campaign metrics)

LAGGING INDICATORS

- **Critical vulnerabilities**
  (On server, client, network infrastructure)
- **Security incidents**
  (By priority)
- **Recorded financial impact**
  ($ impact from cybersecurity incidents)
- **Penetration test results**
  (# of findings in remediation)

Source: Arthur D. Little

ADL Cybersecurity Matrix

From its experience in the development and implementation of cybersecurity strategies, ADL has developed a Cybersecurity Matrix,[1] which breaks down the inherent complexity of the topic for comprehensive understanding (see Figure 6). The framework allows for a deep dive along six cybersecurity domains and six functional areas, each focusing on critical tools or capabilities for coping with the cyber threat landscape.

1 Co-developed with Infinity Grey Ltd on the basis of their Cyber Maturity Model & its embedded Enterprise Cybersecurity Architecture Framework.

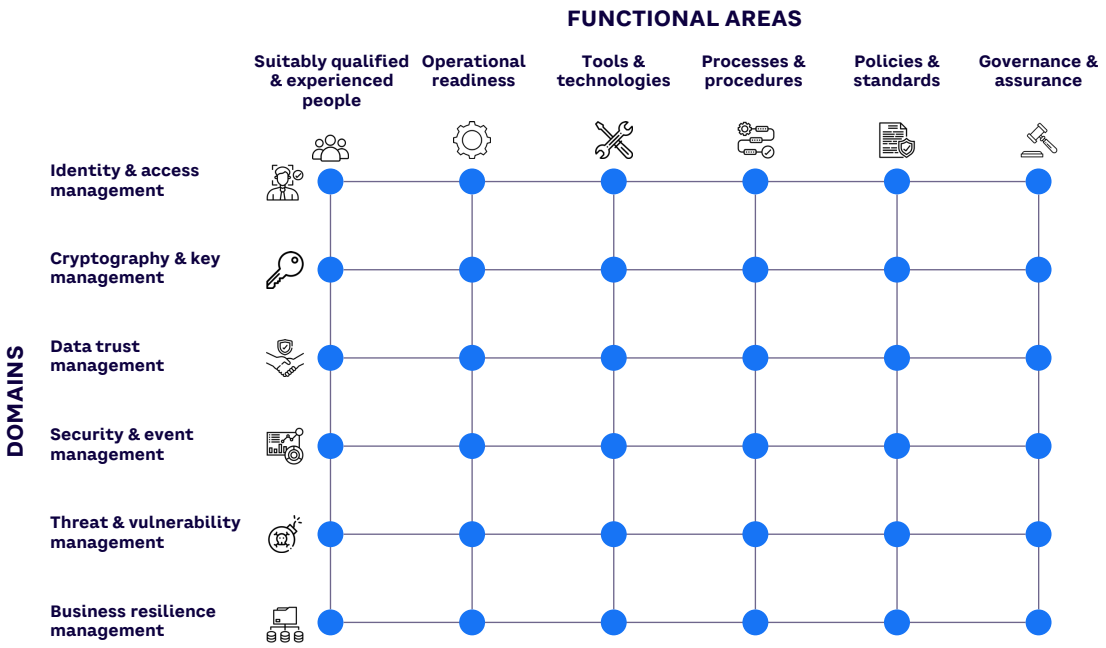
Each intersection in the matrix is given a score based on an expert-led assessment using the Control Objectives for Information and Related Technology (COBIT) maturity model, with maturity definitions ranging from 0 (nonexistent capability) to 5 (optimized capability). This assessment employs a "show me, don't tell me" approach, where each statement from an organization's cybersecurity expert is checked live (e.g., by interviewing company-internal subject matter experts, accessing the firewalls' management console).

Figure 5. Global cybersecurity standards

ISO 27001	A.5 – Information security policies	A.12 – Operations security	18 domains with 32 secondary objectives
	A.6 – Organization and information security	A.13 – Communications security	
	A.7 – Human resource security	A.14 – System acquisition, development, and maintenance	
	A.8 – Asset management	A.15 – Supplier relationships	
	A.9 – Access control	A.16 – Information security incident management	
	A.10 – Cryptography	A.17 – Information security aspects of business continuity mgmt.	
	A.11 – Physical and environmental security	A.18 – Compliance	
IEC 62443	FR 1 – Identification & authentication control	FR 5 – Restricted data flow	7 domains with 51 secondary objectives
	FR 2 – Use control	FR 6 – Timely response to events	
	FR 3 – System integrity	FR 7 – Resource availability	
	FR 4 – Data confidentiality		
NIST	ID – Identify	RC – Recover	5 domains with 23 categories
	PR – Protect		
	DE – Detect		
	RS – Respond		

Source: NIST, ISO, IEC

Figure 6. ADL Cybersecurity Matrix



Source: Arthur D. Little, Infinity Grey Ltd

The framework supports companies by providing the granularity they need to unveil their main pain points, while still offering the measurability and conciseness needed for raising awareness among upper management. It effectively creates a baseline for an organization's cybersecurity program and allows for an actionable plan to ensure that organizations spend cybersecurity budgets on measures with the highest impact.

Creating an action plan to target underperforming areas

The assessment based on the sample Cybersecurity Matrix shown in Figure 7 delivers an average maturity score of 2.8 (defined process). However, it is more important to observe the scores of each domain or functional area. In this sample assessment, Threat and Vulnerability Management is one of the weakest capabilities due to a lack of employees with suitable qualifications, insufficient budgets, largely manual tools, and no regular and defined governance structure to assure key stakeholders of the progress in this capability.

These findings provide an outline for a clear and actionable roadmap for the Threat and Vulnerability Management domain with a focus on increasing FTEs, qualifications of existing staff, assigning additional budget, procuring state-of-the-art tools, and setting up a governance process focused on the domain. Such actions can be defined for each intersection of the matrix to achieve a targeted maturity level across the organization.

The Cybersecurity Matrix based on the assessment delivers a comprehensive set of recommendations to address intersections of the matrix and improve the maturity toward a level targeted by an organization.

Figure 7. Arthur D. Little Cybersecurity Matrix: Sample assessment result

Functional areas / *Domains*	Suitably qualified & experienced people	Operational readiness	Tools & technologies	Policies & standards	Processes & procedures	Governance & assurance	*Avg.*
Identity & access management	3	3	4	3	4	3	3.3
Cryptography & key management	2	3	2	3	2	2	2.3
Data trust management	3	4	4	4	4	3	3.7
Security information & event management	3	3	2	3	3	3	2.8
Threat & vulnerability management	2	2	2	3	3	2	2.3
Business resilience management	3	3	2	2	2	3	2.5
Average	2.7	3.0	2.7	3.0	3.0	2.7	2.8

Each quadrant of the matrix evaluated based on COBIT scale:

0	Non-existent
1	Ad hoc
2	Repeatable but intuitive
3	Defined process
4	Managed and measurable
5	Optimized

Source: Arthur D. Little

CONCLUSION

ADDRESSING CYBERSECURITY AT THE BOARD LEVEL

BOARDS CAN MEASURE, MANAGE, AND COMMAND CYBERSECURITY PERFORMANCE TOWARD A SUSTAINABLE REDUCTION OF RISK

Cybercrime is a growing threat that will require C-level attention in organizations across the globe. We offer four steps boards can take toward establishing fit-for-purpose cybersecurity capabilities:

1. **Engage an objective expert view on the status quo of the organization's cybersecurity maturity.** Ideally, this assessment should ensure the necessary level of granularity while still providing readily understandable insights and priorities for the C-level audience (e.g., ADL's Cybersecurity Matrix).
2. **Ensure regular oversight of the organization's key indicators for cybersecurity performance,** both leading and lagging, providing assurance that the controls in place are offering the right level of protection.
3. **Review fact-based and unvarnished updates on a regular basis.** This not only facilitates progress tracking but also ensures that resources are allocated in the most effective way for reaching the intended maturity level.
4. **Enable the required governance and funding to reach the organization's target state,** based on a dedicated action plan, while ensuring identified vulnerabilities are immediately addressed.

By following these steps, boards can measure, manage, and command cybersecurity performance toward a sustainable reduction of risk.

Arthur D. Little has been at the forefront of innovation since 1886. We are an acknowledged thought leader in linking strategy, innovation and transformation in technology-intensive and converging industries. We navigate our clients through changing business ecosystems to uncover new growth opportunities. We enable our clients to build innovation capabilities and transform their organizations.

Our consultants have strong practical industry experience combined with excellent knowledge of key trends and dynamics. ADL is present in the most important business centers around the world. We are proud to serve most of the Fortune 1000 companies, in addition to other leading firms and public sector organizations.

For further information, please visit www.adlittle.com.