Arthur D Little

Viewpoint

From risk to resilience: Digital defense

Building effective cyber-resilience through an organization-wide approach

There is no doubt that while the world is enjoying the benefits of the fourth industrial revolution, the risks to businesses from cyber-threats are increasing in both sophistication and frequency. What can business leaders do to strengthen their resilience to cyber-threats? Leaders must firstly recognize that the risks in the digital space present as real a threat to the success of the business as the more familiar risks in the physical world do. In the digital world, where actions take nanoseconds and commands are increasingly issued without human intervention, the traditional "measure and manage" approach to risk management is rapidly becoming obsolete; "sense and respond" is a more appropriate approach in the digital age. Attacks are increasing in diversity, frequency and ferocity, which necessitates a challenge to the accepted practice that cyber-risk can be managed within the IT function. To build effective digital resilience, leaders must adopt a C-Suite response, embracing both robust technology and organizational culture approaches.

The cyber-threat landscape

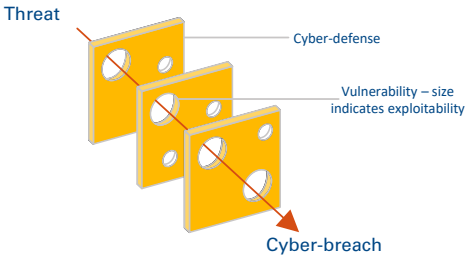
The cyber-threat landscape is evolving at a pace that many boards find difficult to grasp. Agile working, the cloud and the Internet of Things (IoT) shape a threat environment that is truly complex. In today's dynamic digital environment, new threats are emerging and organizations must fend off phishing attacks, DDoS and malware at unprecedented levels – 77 percent of organizations have experienced cyber-attacks in the last year[1].

Threat actors are not always cyber-criminals; they can also include state-sponsored actors and insider threats – both malicious and non-malicious. Threat actors exploit organizations' vulnerabilities, with severity ranging from data loss to physical damage due to loss of control systems. Understanding your organization's position within the cyber-threat landscape is crucial to understanding your cyber-risk profile: organizations holding valuable information assets (e.g., customer data, financial transactions) are high-value targets for threat actors.

Poor threat perception decreases protection

The gap between the perception and reality of threat widens higher up the leadership chain, with many executives and board members largely unaware of the threat landscape in which their organizations exist.

Cyber Swiss Cheese Model



Source: James Reason, Arthur D. Little

A recent study highlighted that **"43 percent of senior executives believe their organization detects all cyber-threats, whereas only 17 percent of non-executives do[1]"**.

Cyber-risk is a function of the threat posed, the system's vulnerabilities and its exploitability, as illustrated by the cyber Swiss Cheese Model. A vulnerability can be defined as a weakness in the system, and its exploitability as the likelihood of it actually being exploited. Reducing the exploitability of an organization's vulnerabilities and improving their cyber-defenses decreases the likelihood of a cyber-breach.

Eighty-seven percent of FTSE 100 organizations stated in its 2017 annual report that they had cyber-risk controls, but only in recent years had senior leadership begun to recognize

1 Business Wire, 2017

cyber-risk as a core business risk[2]. This has resulted in a lack of organizational capability to protect against, detect, respond to, and recover from cyber-incidents. Failure to recognize the threats that their organizations face leads to **passivity and complacency**, which **is likely to result in increased cyber-risk**.

Digital damage

Impact from a cyber-attack extends far beyond the digital domain. An organization experiencing a cyber-breach can suffer devastating reputational damage and financial losses. A holistic threat, such as a malware infection or server failure, can result in virtual impact such as a data breach or operational loss. It can also cascade into physical effects, with potential for death in hazardous industries such as oil & gas, transport and utilities.

The reliance that businesses place on their digital platforms is ever increasing. The common view that "as long as everything works, there are no problems" is inherently flawed. Any successful business has comprehensive understanding of physical or human assets that are critical for it to be both successful and resilient, so why is its digital backbone, which is at least as critical as any other asset, so widely ignored? Senior leadership tends to operate in a different world from the IT team, which runs the digital services, yet there is a critical need for improved **understanding of business-critical assets and the dependency that critical business processes have on them,** to ensure there is a robust cyber-security risk management framework.

The "scatter-gun" approach to protecting everything within an organization leads to a false sense of security due to a perception of comprehensive protection, which is impossible. Substantial digital damage occurs when critical assets are compromised; it is imperative that senior management develops early and clear understanding of these.

In 2017, the WannaCry ransomware attack infected thousands of British health service computers, causing huge disruption. The information systems that shared data between geographic regions and hospitals were severed. Management failure to implement a software update several months prior was to blame. Failure to perceive the potential threat, and subsequent significance of that threat, led to the ransomware infection. This highlights how damage caused within one business unit can have a knock-on effect on the whole organization.

The new General Data Protection Regulation (GDPR) within the European Union imposes severe penalties for organizations that fail to protect their data assets (the higher of 4 percent of annual turnover or €20m). Organizations must report data breaches within 72 hours, which puts pressure on operations and IT systems to ascertain what information has been compromised in a short time frame.

Organizations underestimate the potential loss from a cyber-breach due to over-reliance on their IT functions to protect them and overconfidence in their ability to detect cyber-attacks early. So what steps can organizations take to improve this?

Case studies

Cyber-attacks often go unreported in the media due to organizations wishing to avoid negative publicity. Those reported generally lack awareness of the risk at a leadership level, which has resulted in both virtual and physical impact. Two notable examples are:

Saudi Aramco, 2012

National oil company (NOC) Saudi Aramco was hit by a catastrophic cyber-attack in 2012. A phishing email was sent before the public holiday of Ramadan to decrease its chance of detection, and infected 30,000 computers with the Shamoon virus. A corporate blackout occurred as the company's electronic systems were disconnected, with phone lines ringing dead and emails offline. Sales systems were inaccessible, and after 17 days oil was given away for free to avoid ceasing production. The company's recovery time from the incident was over two weeks, which caused significant disruption to Saudi Aramco as one of the world's largest oil producers. Costs ran to hundreds of millions of dollars, with Saudi Aramco having to destroy and replace all corrupted hard drives. The attack was attributed to an employee opening the phishing email, which indicates a need for employee vigilance.

Ukraine Utilities, 2015

A cyber-attack on the Ukrainian power grid in 2015 left 225,000 customers without power for up to six hours. Malware gained access to the company's computers and industrial control systems, disconnecting substations and disrupting the power supply. The attack was well planned and had started six months prior to the blackout, which highlights the need for early detection of any cyber-incident. The event was attributed to a state-sponsored phishing attack by the Russian security services, which highlights the potential for powerful state attacks on critical national infrastructure companies.

Transformation: From risk to cyber-resilience

Elsewhere[2], we have discussed how many companies are employing more traditional technology approaches or more audits to address the rise in cyber-risk, along with the shortcomings of these approaches and the need to integrate both technological and risk management approaches into holistic solutions.

2 Arthur D Little Viewpoint – Cyber-threat: Is your business prepared?

In the following section we discuss specific issues with the traditional technological approaches used to combat cyber-risk and the critical role of culture and leadership in building resilience throughout the organization.

Traditional cyber-risk management focuses on "hardening" the perimeter with firewalls or antivirus software to protect assets. However, the digitally connected world means simply building a "hard shell" around the business is not enough to ensure cyber-resilience. Identifying, as well as understanding, business-critical assets is essential to protecting them. The increased interconnectivity of such assets to a global company network, and ultimately the internet, makes this more difficult. Organizations must engage with management at all levels across business functions to identify and understand their businesses better. The C-Suite has to engage as cyber-leaders of the organization, moving away from the philosophy that cyber-security is only the concern of the IT function, as well as developing a business-led – rather than technology-led – approach to managing cyber-risk.

Our research shows that while technical barriers reduce the likelihood of threat penetration, there is significant residual chance that a threat could still exploit an organization's vulnerabilities. Investing heavily in the "hard shell" can potentially cost more than it saves through reduced losses from cyber-breaches. A more internally driven approach from within the organization is required. Focusing digital defenses outside the business perimeter limits the scope to which an organization can both detect threats and protect its business-critical assets, as many threats arise from within the business.

The "tick box" risk management approach of having certain "hard shells" can no longer be relied upon as a measure of cyber-security and the risks that organizations face. We have created the C-Suite Cyber Culture Model, which aims to help the C-Suite use a holistic cyber-risk framework for the business.

This alternative is known as cyber-resilience, and must stem from an organizational response to cyber-risk at the C-Suite level. This requires stakeholder engagement, recognition of cyber-risk as a core risk that affects all business functions, and the use of both human and technological strategies. The diagram below illustrates the transformation from risk to resilience.

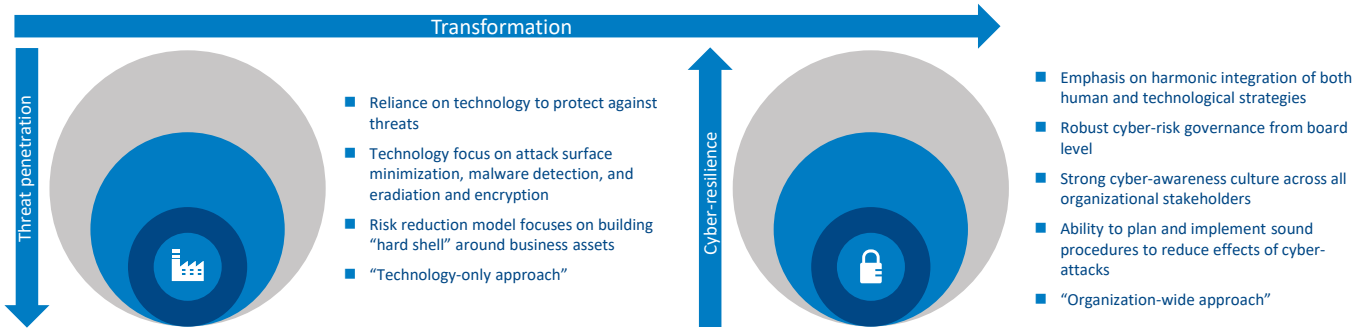
Resilience is built on, and can be monitored against, five categories:

- **C-Suite Cyber Culture (CCC) Model** – cyber-awareness and culture within the organization that comes from top-level management.
- **Vendor cyber-security** – management of contractors, third-party procurement and all IoT devices.
- **IT management** – management of information technology applications in general operations and capacity management.
- **IT security** – both human and technological aspects of cyber-security breaches.
- **Data governance** – the security and integrity of an organization's data and information assets.

But how does the C-Suite know if it is worth transforming into a cyber-resilient organization? Key risk indicators (KRIs) and key performance indicators (KPIs) allow the C-Suite to measure performance at executive level. We have developed a set of relevant KRIs and KPIs to apply within an organization to build up a cyber-risk dashboard for the C-Suite to review their performance. Evidence suggests that building resilience stems from top-level strategies and governance to provide an organization-wide approach of embedding cyber-risk within strategic risk oversight.

Continuous monitoring and improvement are vital for early threat detection and prevention. They also enable identification of underlying causes of risk exposure and refinement of the selection of appropriate leading KRIs. Organizations must adopt a proactive view to retaining key business knowledge of cyber-operations, reviewing and responding to new developments both internally and externally, and always aiming for continuous improvement.

C-Suite Cyber Culture (CCC) Model



Source: Arthur D. Little

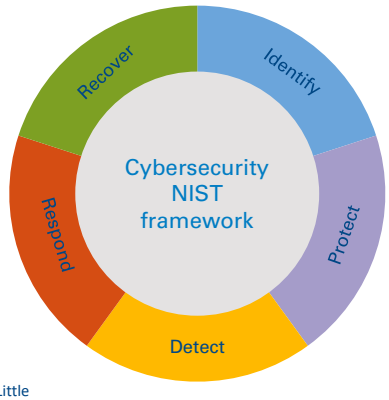
Arthur D Little

Viewpoint

The National Institute of Science and Technology (NIST) Cybersecurity Framework provides a starting point against which organizations can benchmark their digital defenses. In our view, this has to be expanded to determine the total cost of risk (TCoR), using a combination of the NIST framework, scenario modeling and root-cause-and-effect analysis. "Bowtie" analysis, a widely established risk management technique, builds on the NIST framework to provide a more in-depth risk management view and support, building cyber-resilience from within an organization.

By combining these to calculate the TCoR, we can develop robust risk mitigation controls aimed at managing the costliest risk scenarios to optimize reduction of financial losses, protect reputation, and improve overall performance. Furthermore, a reliable assessment of the TCoR, supported by an appropriate suite of leading KRI metrics, can be used to demonstrate risk reduction to insurers and verify that insurance premiums truly reflect the residual risk that remains.

Risk mitigation controls



Source: Arthur D. Little

Insight for the executive

Cyber-risk has increased dramatically for organizations, and senior leaders must do more to put up their digital defenses. This risk is not "around the corner" – it is present and increasing. Our key conclusions on transitioning from cyber-risk management to cyber-resilience are:

- Adopt a C-Suite cyber-culture.
- Change the company mind-set from reliance on technological defenses to an organization-wide resilience approach.
- Use relevant KRIs and KPIs to review and continuously improve digital defenses.
- Develop robust understanding of the TCoR to support targeted efforts to optimize risk exposure.

By adopting a resilience-led approach to cyber-risk, organizations can increase asset protection and reduce business losses.

Contacts

Tom Teixeira, Partner
teixeira.tom@adlittle.com

Marcus Beard, Associate Director
beard.marcus@adlittle.com

Jamie Gale, Partner
gale.jamie@adlittle.com

Authors

Tom Teixeira, Immanuel Kemp and Marc Fitchett

Arthur D. Little

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** or **www.adl.com**.

www.adl.com/DigitalDefense