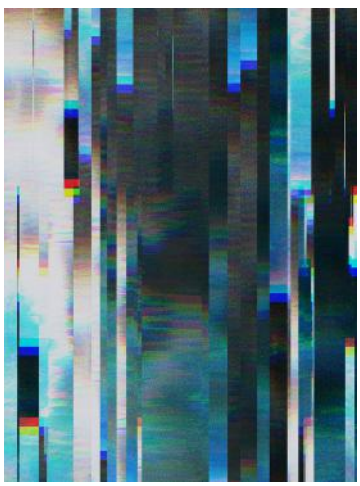
Cyber-threat: Is your business prepared for an attack?

Tom Teixeira, Jamie Gale, Mandeep Dhillon, Immanuel Kemp

Despite the emphasis on and investment in cyber-security, traditional approaches, which tend to focus on either technology or risk, are failing to protect businesses and their customers. This article explains the benefits of adopting a new, unified approach that brings together technology and risk management processes. It enables organizations to better protect themselves against cyber-threats, thus safeguarding their businesses, data and revenues.

As constant news stories demonstrate, traditional approaches to cyber-security and risk are not protecting businesses or their customers. This is not for lack of focus on the subject. After all, no chief executive wants to find themselves facing fines of 4 percent of global turnover under the general data protection regulation (GDPR) in Europe, as negative front-page news, or having to answer regulators' questions about how they were attacked, why they didn't know it was happening, or what they have lost.



This external impact is matched by internal and financial consequences, which affect trust in the brand, value in the company, and loyalty of their most prized assets, their customers. In more extreme cases, such as with AP Moller Maersk[1], costs can rise to over $200 million, or lead to business failure, as in the case of Altegrity[2] after the details of 25,000 members of the Homeland Security department were stolen. Figures show that only 38 percent of global organizations claim they are sufficiently prepared to handle a sophisticated attack[3], despite approximately $1 trillion expected to be spent globally between 2017 and 2021.

The rate and complexity of attacks continues to increase – however, traditional approaches are not keeping pace. This is because they tend to focus on either technology (as sold by technology vendors and large systems integrators) or risk (as sold by risk management firms).

1. https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html
2. https://www.wsj.com/articles/altegrity-files-for-chapter-11-bankruptcy-1423446150
3. www.cybintsolutions.com/cyber-security-facts-stats/

In this article we will explain how a new, unified approach that combines technology and risk management processes can enable organizations to better protect themselves against these cyber-threats, safeguarding their businesses, data and revenues.

The evolving threat landscape

There are two trends in the threat landscape, both of which substantially impact risk:

1. An increase in the frequency of unsophisticated attacks

Cyber-attacks rose by 27 percent in 2017, with an average cost of $12m, and according to AT&T, 323,000 new strains of malware are discovered each day.[4] That equates to three strains per second. Arguably, unsophisticated attacks have never been easier. In many countries, it is not illegal to hire a hacker, and there are no international legal agreements which would make it possible to prosecute cyber-criminals transnationally. At the same time, the Dark Web has become a channel for anybody (inside or outside an organization) to buy, download and deploy malware.

2. New, more sophisticated threats are emerging

Other forms of attack are becoming more sophisticated. As the internet evolves, and cloud computing and the Internet of Things become increasingly commonplace, new opportunities for cyber-criminals open up. Examples include:

- Voice fraud: Consumers make 100 billion calls per month to enterprises, with trillions of dollars of transactions made over the phone. Criminals are targeting this channel, stealing $10 billion a year by attacking call centers, impersonating genuine customers.[5]

4. Bindu Sundaresan – AT&T Cybersecurity Solutions. Masters of Scale Podcast 22 Oct 2018
5. Voice interface is the future – https://tech.co/future-10-billion-voice-fraud-industry-2017-05

- Crypto-mining: Businesses have already reported being attacked by malware that infects their systems to create armies of cryptocurrency-mining machines. This consumes significant computing power at high cost, and acts as a launchpad for other attacks designed to steal intellectual property.

Traditional approaches have not protected businesses

Against this backdrop of increasing threats, businesses have tended to follow a binary approach – deploying more technology or external audits. While these may deliver some benefits, neither has helped clients understand the real impact of cyber-risk to their businesses.

More technology and use of traditional technology practices

Powerful security tools have entered the market as vendors have invested heavily to battle cyber-criminals. However, despite these advances, the basics are often ignored. For example, the infamous WannaCry[6] attack could have been minimized if more organizations had applied best practices, such as patching and setting appropriate incident response processes. Figures from Cisco showed that 93 percent of organizations had experienced security alerts, yet 44 percent of these had not been investigated.[7] And of those that had been investigated, almost half had not been dealt with, and those companies had been left vulnerable and exposed. Clearly, technology alone is not the answer – businesses need to realize that cyber-risk is also a human problem.

6. WannaCry cyber attack and the NHS, https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/
7. https://blogs.cisco.com/security/cisco-2018-annual-cybersecurity-report

On 27 June 2017, the IT systems of multinational conglomerate AP Moller Maersk were affected by the NotPetya malware, which exploited security vulnerabilities in Windows and disabled IT systems across multiple sites and business units.

The recovery effort required 4,000 new servers, 45,000 new PCs and 2,500 applications, and took 10 days to implement, during which time staff reverted to manual systems to continue operations.

Maersk has estimated that the attack cost between $250 and $300 million in lost revenue due to disrupted operations across all its businesses.

The NotPetya malware attack has since been recognized as the largest cyber-attack in the history of the internet, with total worldwide impact estimated at over $10 billion.

More external audits

Understanding your organization's cyber-threat exposure has relied on sub-optimal, lengthy, and tedious questionnaire-based processes. These are resource intensive, requiring a small army of people to carry out the checks. At best they provide static, point-in-time vulnerability assessments, ignoring the increasing frequency and sophistication of attacks.

Additionally, this approach is the key source of "anec-data" – human interpretation of events, which is inevitably subjective and becomes disproportionately important relative to the real data. Essentially, businesses can be fooled into feeling safe as this has given them an audit process.

Neither of these approaches enables businesses to truly quantify and mitigate the financial impact posed by these attacks. In today's sophisticated world, organizations therefore need to adopt an integrated view that combines active threat prevention, total cost of risk models, and a shift in mind-set that is fit for the digital world.

A new, holistic approach to cyber-risk

Given that traditional responses to Cyber-threats have been ineffective and risks are increasing, simply doing more of the same is not enough. A new approach is needed that successfully brings together technology and risk management to focus upon:

- A data-led method which can rapidly and continuously identify anomalies and attacks.
- Clarity of business risks and their underlying causes and impact, along with a means of mitigating financial and reputational consequences.
- Evolving the operating model and mind-set in order to protect the long-term interests of the company and its customers.

Businesses understand the inevitability of future attacks. With this new approach, they are better positioned to protect themselves. They can first identify vulnerabilities and related exposures early, and then prepare themselves due to clarity over the prioritized pragmatic steps that can be implemented in advance to support reduction in the overall total cost of risk (TCoR).

Key definition:

Total cost of risk (TCoR) is a data-led approach to assessing the financial impact of risk. This allows active prioritization of remediation activities related to business value.

We use it with cyber-risk to understand which risks are manageable internally, and which have such severe impact that some of the financial risk needs risk-transfer solutions, such as insurance.

Underpinning this new approach are three central themes:

1. Defining the total cost of risk

Traditionally, much cyber-risk analysis has focused on technical vulnerabilities. While these have then found their way onto risk registers at board level, their wider business impact has not been codified, and this results in little understanding of the levers that can be used to reduce the TCoR.

The TCoR calculation should be unique to every organization, dependent on its circumstances and priorities. However, the key dimensions remain consistent:

a) Costs of consciously retaining risks, which incorporate the likely cost of claims and earnings volatility.

b) Costs associated with controlling risks, such as re-engineering, value/supply chain risk management, and the management of continuity plans.

c) Costs associated with new technology implementations and capability development.

d) Costs of transferring risks through additional insurance premiums and associated administrative costs.

e) Any internal and external risk management costs in the areas of human resources, treasury, audit, quality, etc., and the additional administration associated with these new dimensions.

The "assess" phase provides the necessary data for businesses to select the right risk exposure scenarios, based on vulnerability and frequency, or whatever the threat may be. For each scenario, a set of assumptions is co-created, and this provides a base financial case for each risk. This means understanding the size and scale of the potential threats, as well as the corresponding potential size and scale of the opportunity.

The executive team and board now understand aspects of impact, and can factor these into their financial planning, forecast models and cash flows. Essentially, they have the tools to leverage the upside of risk while mitigating the downsides.

2. Using technology and data to rapidly and continuously assess the threat landscape

Most large organizations have mixed technology estates combining cloud computing, on-premise and hybrid environments. Understanding the exposure level across all areas of infrastructure and applications is important. Deployment of physical devices on the network, such as router plug-ins, or deployment of software agents, such as user activity monitoring and next-generation firewalls within the technology estate, can and should be rapid (i.e., within a day). This enables organizations to begin gathering insight within hours, rather than days or weeks.

The San Francisco Municipal Transport Agency's (SFMTA's) computer systems were infected by ransomware in 2016.

Although trains remained running, the SFMTA had to open all ticket barriers, which cost $50,000 in revenue over the weekend. Fortunately, the attack did not compromise passenger safety, although future attacks could target train signaling, which could cause delays or even derailment.

An investigation determined that an employee had opened a phishing email, which had resulted in covert installation of the ransomware. Lack of investment and aging systems had contributed to the organization's increased vulnerability to such an attack. This highlights the importance that senior leadership must place on having a strong cyber-security culture, adequate resourcing and robust infrastructure within the organization.

Rather than a "point-in-time" approach, these sensors and agents provide a continuous threat assessment capability. This means they will therefore not only continue to highlight new and emerging threats and vulnerabilities, but also begin to highlight changes in behavior of internal staff. Rapid implementation of appropriate technology solutions is important for two main reasons:

- Properly deployed and used, these tools go a long way towards protecting your organization.

- They can be used to help identify the underlying causes within risk exposure. This, in turn, will help identify leading key risk indicators (KRIs), which can be used to demonstrate to insurers that scanning mechanisms are in place. These aim to reduce risk by applying the right level of resources at the right time.

Alongside a set of these KRIs, insurers can analyze actual data and build findings into the limits and triggers associated with insurance policies and premiums charged to an organization. Working collaboratively and transparently with the insurer in this way can provide organizations with financial benefit in terms of realistic premiums and improved coverage, as relevant scenarios are incorporated into the wording. Ultimately, it should reduce the volatility of future earnings.

3. Ensuring the right technology operating model is in place

Human and organizational elements can be barriers to safeguarding a business. Failure to address these factors will lead to little improvement in your ability to prevent attacks. Instead, understand the "seven voices of technology"[8] to highlight the tensions and weaknesses within internal operations. (See Figure 1.) For example, where the change team has a more dominant voice than that of operations,

8. Source: Greg Smith, Arthur D. Little

technology can be implemented without necessary controls being in place. Documenting these tensions and rebalancing the "voices", alongside establishing a set of leading, rather than lagging, KRIs, will begin to drive a cultural and mind-set shift within the organization. This addresses an issue often missed by traditional approaches.

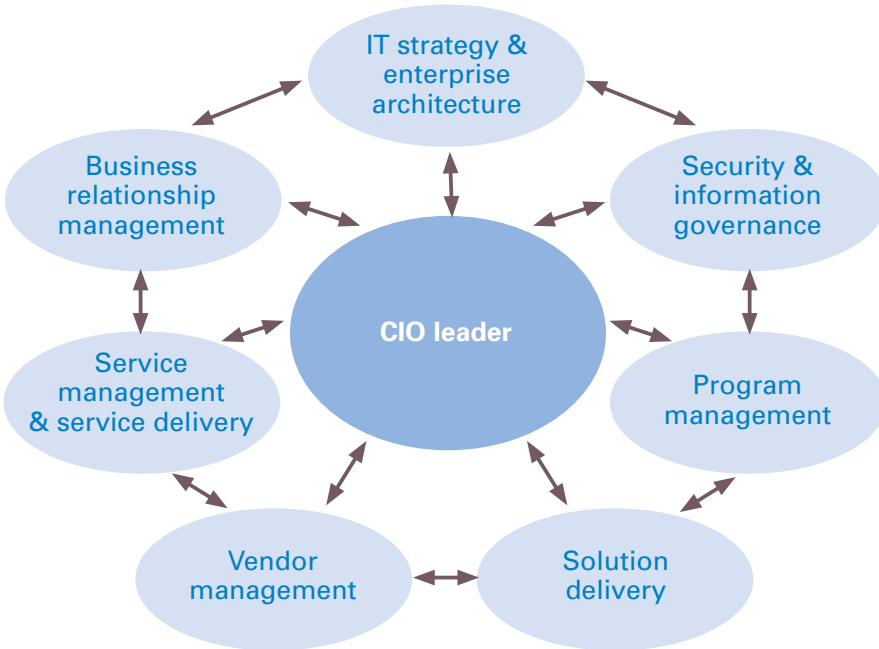


Figure 1: The seven voices of technology

It is critical to understand and address the perception and capability gaps between what the executive team believes is reality and what the operational assessment and data demonstrate to be the case. An example of this is around tolerance of failure. An executive team may believe that the company has robust plans to deal with failure, but the data associated with its technology or supply chain may show otherwise.

The benefits of taking this approach are:

- It drives quick results and does not require armies of consultants performing tick-box exercises. It delivers rapid, actionable results, which means quickly identified threats can be fixed, controlled or sandboxed. In addressing these first threats, it removes the tension between whether to focus on the urgent or the important.

- It is data-led, which means decisions are made around facts, not anecdotes. It is designed to be a sustainable way to assess threats, rather than to provide a point-in-time audit.

- Ultimately, it provides the executive and board with a business-led, rather than technology-led, set of issues and recommended solutions. This highlights ways of reducing the TCoR that are designed for that organization, and extends beyond a large, but potentially ineffective, technology implementation.

Insight for the executive

With cyber-threats increasing, as well as sophistication and impact, organizations require a better way of managing these risks.

Investing the vast sums spent on cyber-security more effectively than has been done to date will be key. CEOs therefore need to change approach and focus on a more holistic method that brings effective use of technology together with risk management. Following this three-stage process will give them the tools to prepare operationally and financially for cyber-risks:

- Assess and address. Use technology to uncover and deal with immediate threats in a way which is sustainable over time, while defining the organization's total cost of risk.

- Plan and analyze. Carry out financial and operational analyses, based on real data, to inform the executive team so they can create a pragmatic plan that reduces the TCoR.

- Do. Act on your plan, such as by transferring elements of risk to insurance markets, creating appropriate internal controls linked to key risk indicators. Overall, look to create a mind-set that supports perpetual preparedness.

Tom Teixeira
is a Partner at the London office of Arthur D. Little and a member of the Risk Practice.

Jamie Gale
is a Partner at the London office of Arthur D. Little and a member of the Digital Problem Solving Practice.

Mandeep Dhillon
is a Principal at the London office of Arthur D. Little and a member of the Digital Problem Solving Practice.

Immanuel Kemp
is a Consultant at the Cambridge office of Arthur D. Little and a member of the Risk Practice.