Building cyber-resilience to tackle threats

Michael de Crespigny

Michael de Crespigny, Information Security Forum (ISF)

Business leaders recognise the huge opportunities and benefits offered by cyberspace in terms of increasing innovation, collaboration, productivity, competitiveness and customer engagement. Yet the threat from 'malspace' – an online environment inhabited by hacker groups, criminal organisations and espionage units – is growing and developing daily. How can organisations strike a balance between the risks and rewards and prepare effectively to counter the growing threats from cyberspace, without losing the potential benefits?

Cyberspace is critical to organisations today – from the supply chain to customer engagement – and slowing adoption or disconnecting from cyberspace is simply not an option. However, the commercial, reputational and financial risks that go with cyberspace presence are real and growing, driven by two key factors.

First, cyber-criminals are now better organised and more professional in their approach. They innovate just as business does, and the financial rewards for them grow as business use of cyberspace grows. They also have access to powerful online tools and expertise for identifying, targeting and attacking their victims, and online markets to launder their booty.

Second, cyberspace is constantly evolving and presenting new opportunities. The desire of businesses to quickly adopt new technologies – using the Internet to open new customer channels and adopting cloud and other online services – provides enormous opportunity, but also brings with it unforeseen risks and unintended consequences that can have a negative impact on a business.

> ***"It's time for us to start collaborating as effectively as the bad guys are"***

All the benefits that cyberspace confers on legitimate organisations – better collaboration and innovation, faster execution, global connectivity – are also available to hackers and attackers. Every hacker group, criminal organisation and espionage unit in the world has access to increasingly powerful and evolving capabilities – illustrated in Figure 1.

Exploiting the potential of cyber is a given, but dealing with the cyber-threats is an issue for the whole organisation, not just the information security function. As one Information Security Forum (ISF) member put it: "It's time for us to start collaborating as effectively as the bad guys are." So how should organisations address the issue?

The 10 key challenges

In its recently published report, 'Cyber Security Strategies: achieving cyber-resilience', the ISF identified the 10 key challenges involved in balancing the risks and rewards of cyberspace, based on insights from the organisation's global membership and its own research.[1]

- The benefits and risks of cyberspace are huge, and the benefits continually drive organisations and employees to adopt new ways to interact and do business online. However, they must be able to do so quickly and securely, while managing the risk to deliver the rewards.
- No-one is safe from attack, so apart from taking appropriate steps, organisations

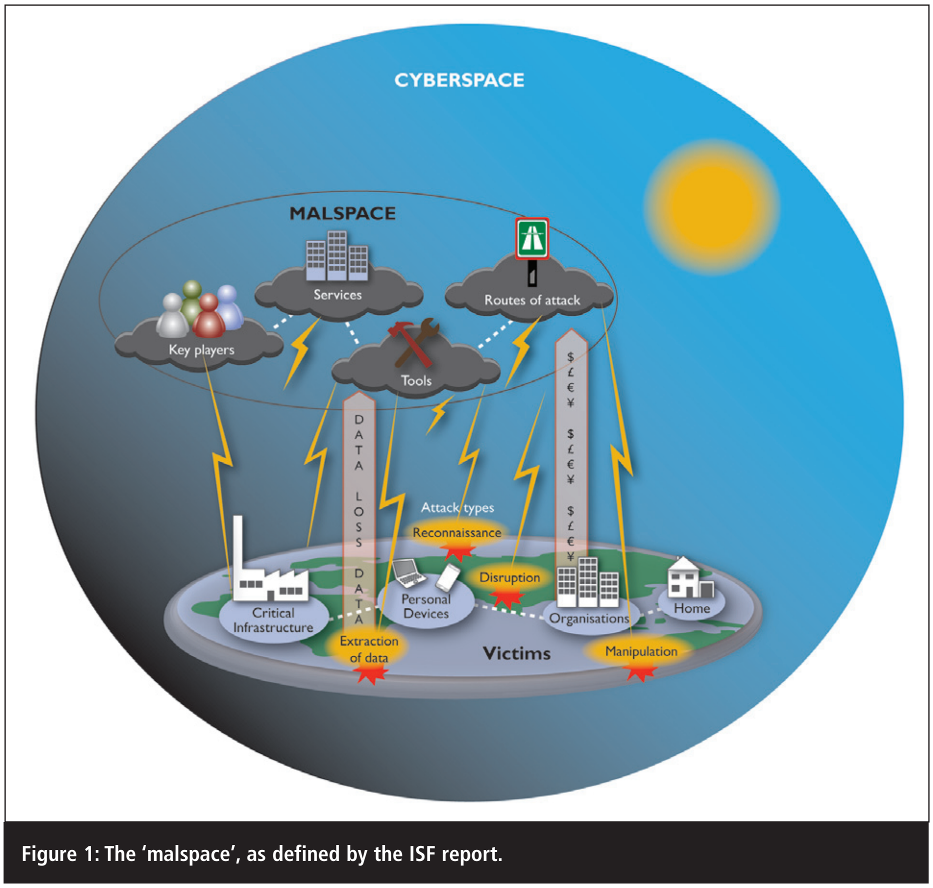

Figure 1: The 'malspace', as defined by the ISF report.

must embrace uncertainty and develop what might be called ‘cyber-resilience’. The pace of evolution and potential impacts from cyber-criminals are so large that traditional enterprise risk management is now insufficient to deal with it.

- ISF has coined the term ‘malspace’ to reflect a global industry that has evolved to facilitate cybercrime. Malspace is a large, highly functional industry that supports all aspects of modern crime – the development and sale of sophisticated attack tools, services and large-scale laundering of stolen assets. It operates at the scale, and with the sophistication, of other global industries.
- The impact of cyber-threats can be a very long and disproportionate ‘risk tail’ – for example, a data breach from years ago can be a ‘sleeping giant’ that can be recalled or reawakened at any time. Incidents and criminal rewards are also magnified in cyberspace, making the impact of even moderate incidences disproportionately large.
- Hacktivism also presents significant threats to the organisation. While some forms may be lawful – viral videos, blogs, boycotts, email campaigns and petitions – hacktivism in all its guises can have a negative impact on targeted organisations.
- Cyber-security is much more than just information security. While the information security function has many of the skills needed to address cyber-threats, the organisation needs to hone additional skills to lead the charge to improve both its cyber-security and cyber-resilience.
- Cyberspace vastly increases information security risk. Threats to information security are much greater because cyberspace reduces the risk of criminal perpetrators being apprehended. It facilitates collaboration, provides powerful weapons, concentrates targets and provides a shroud to hide what might come next.
- Information security is fundamental to cyber-resilience. Most cyber-threats are to the Confidentiality, Integrity and Availability (CIA) of information and systems. Information security fundamentals – including controls, standards, encryption and governance – are therefore core to addressing threats from cyberspace.
- The complexity of cyberspace enables threats to combine in unpredictable and dangerous ways. Just as it would have been difficult to predict the rise of Anonymous or LulzSec, it is difficult to predict what might emerge from cyberspace next.
- When it comes to building cyber-resilience, there is widespread recognition that safety and business success cannot be achieved in isolation. It is essential to collaborate, share intelligence and develop best practice. Organisations, led by their information security function, need to team up with other functions internally, and with external stakeholders – customers, suppliers and independent bodies – to share knowledge and strategies in order to build resilience.

With unpredictable, and sometimes unpreventable, cyberthreats emerging overnight, traditional risk management is no longer agile enough to deal with the potential impacts from cyber-criminal activity. So, how can organisations develop cyber-resilience so that they can anticipate and respond to the threats head-on, while building on their existing security practices and infrastructure? What are the key capabilities needed to enhance security posture and protect business interests against ever-evolving cyberthreats?

Taking the broader view

There is considerable value in adopting a broader view of cyber-security that includes all aspects of an organisation’s presence in cyberspace – in fact, it is critical to longer-term success. This ‘big-picture’ approach should encompass non-traditional, non-CIA related threats to organisations in cyberspace, including hacktivism, unintended consequences of careless but legitimate data release, and unintended consequences of using cyberspace.

Cyberspace gives criminals and hacktivists power and reach they have not had before, so that even when attacks are not on information CIA, there are significant negative business impacts for organisations. By combining information from various data sources, targeting organisations that process data, or downloading database scraping tools, cyber-criminals can retrieve, match and correlate information that was never intended for release. For example, by tracking corporate aircraft flight plans, competitors might discover commercial or merger talks. And a classic example of an unintended impact from the use of cyberspace is when a seemingly innocuous email gets misinterpreted, forwarded and goes viral – spreading quickly, damaging reputations and potentially affecting share price.

“Cyber-criminals can retrieve, match and correlate information that was never intended for release”

Taking a broader view of cyber-security acknowledges that threats to information and systems in cyberspace are magnified. The impact on an organisation can now be orders of magnitude larger than it was just a few years ago, making the initial incident almost trivial by comparison. One example of this is the impact from targeted threats. The day after WikiLeaks threatened to ‘take down’ a major bank, one bank’s shares fell by 3%. The data release was just a threat – WikiLeaks didn’t actually post any data. The identity of the ‘targeted’ bank was just a rumour – WikiLeaks didn’t say which bank’s data it allegedly held. That didn’t stop the bank’s share price from falling, nor did it stop the bank from invoking a crisis response team and incurring significant costs and disruption, tying up resources and engaging external advisors and lawyers.

While attacks threaten information CIA, the motivation for an attack can also be ideological rather than profit-driven. This means organisations that might otherwise be immune from attack could now be a target, and if the organisation isn’t paying attention, the threat could be missed – undermining the organisation’s focus or ability to respond.

With data more easily available and exchanged than ever before, there are growing cases of unintended releases of information. In one recent case, an investigations company released a public report that was, unfortunately, an edited version of another, confidential report. The document metadata included enough information to tip off an organisation and individuals that they were being investigated.

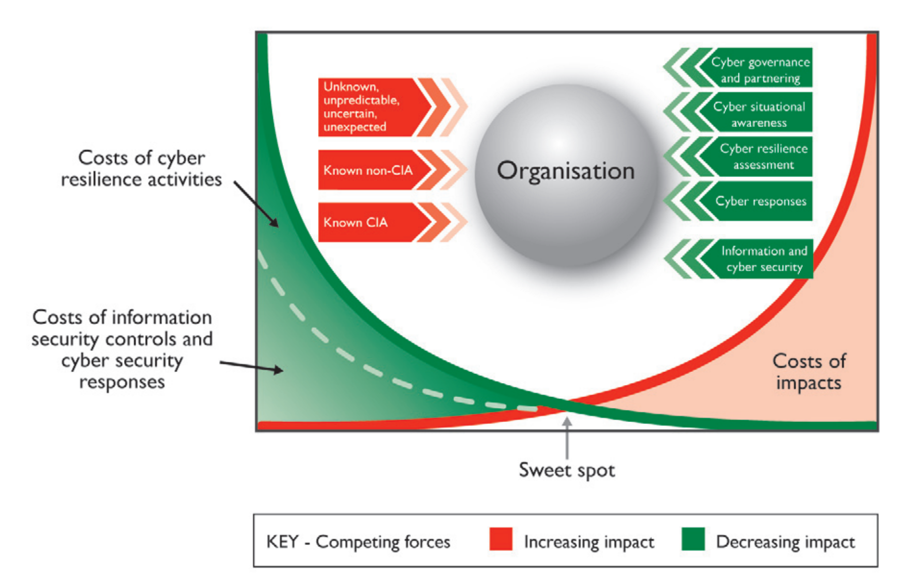
Costs of cyber resilience activities
Costs of information security controls and cyber security responses
Unknown, unpredictable, uncertain, unexpected
Known non-CIA
Known CIA
Organisation
Cyber governance and partnering
Cyber situational awareness
Cyber resilience assessment
Cyber responses
Information and cyber security
Costs of impacts
Sweet spot
KEY - Competing forces
🟥 Increasing impact
🟩 Decreasing impact

Figure 2: The cyber-resilience sweet spot.

"It requires the commitment and guidance of C-level executives – it is no longer purely a job for the information security function"

Finally, adopting a broader view of cyber-security acknowledges the potential of crime in cyberspace, which facilitates and 'de-risks' criminal activity for the perpetrators – obscuring their location and shrouding future activities. By concentrating the targets in one place – the Internet – criminals can more easily collaborate and deploy powerful weapons to attack organisations, systems and people.

From cyber-security to cyber-resilience

Organisations need to become much more cyber-resilient. They need to extend their risk management focus from information CIA to include other risks, such as those to reputation and customer channels, and recognise the unintended business consequences from activity in cyberspace. It requires the commitment and guidance of C-level executives, as well as new levels of collaboration and co-operation across different business units and functions – it is no longer purely a job for the information security function.

Tackling cyber-security alone is not enough either. Today, risk management largely focuses on achieving security through the management and control of *known* risks. The rapid evolution of opportunities and risks in cyberspace is outpacing this approach and it no longer provides the protection required. Organisations must extend risk management to include risk resilience, in order to manage, respond and withstand any negative impacts of cyberspace activity.

A number of headline-grabbing, low-probability, high-impact events have dominated board and risk committee agendas recently. These events have created the realisation that some critical, high-impact risks cannot be anticipated and mitigated in a traditional way. As former US Secretary of Defense Donald Rumsfeld famously put it in 2002: "There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know." He was referring to the situation in Iraq, but the statement applies just as well to the threats organisations face in cyberspace. The inability to eliminate the 'unknown unknowns' in cyberspace is what makes this focus on cyber-resilience so important.

Degree of uncertainty

Cyber-resilience anticipates a degree of uncertainty: it's difficult to undertake completely comprehensive risk assessments about participation in cyberspace. It also recognises the challenges in keeping pace with, or anticipating, the increasingly sophisticated threats from malspace. It encompasses the need for a prepared and comprehensive rapid-response capability, as organisations will be subject to cyber-attacks regardless of best efforts to protect themselves. Most importantly, cyber-resilience is about ensuring the sustainability and success of the enterprise, even when it has been subjected to the almost inevitable attack.

"Hitting the cyber-resilience 'sweet spot' requires investment based on high-quality cost data about the controls, responses and impact of incidents"

The challenge is to ensure there is balance between the cost of controls, responses and other cyber-resilience activities against what would have been the spend to minimise the cost of attacks from cyberspace, as shown in Figure 2.

Hitting the cyber-resilience 'sweet spot' requires investment based on high-quality cost data about the controls, responses and impact of incidents – and the ability to anticipate the consequences of attacks against the organisation. It is hard to know whether organisations have sufficient history or cost information to model this. As experience emerges, providing guidance on assessing this sweet spot will develop into a more exact science. In the meantime, ISF has developed a diagnostic tool to help organisations understand their level of cyber-resilience.

Sharing knowledge

A key finding of the ISF cyber-resilience report is that no organisation can respond effectively on its own to the threats from cyberspace. Organisations must work with others to leverage the knowledge and resources of numerous stakeholders. This will both help to prevent attacks (or minimise their impact) and improve cyber-resilience.

Organisations will also benefit from partnering with others by sharing intelligence and influence the adoption of best practice across cyberspace. Partnering activities should help continually improve collaboration; the quality, usability and trustworthiness of intelligence; and connections to, and engagement with, regulatory developments. In addition, organisations should apply the same partnering approach internally, sharing knowledge and best practice across business units and functional groups.

The concept of intelligence sharing and partnering, both within an organisation and outside, forms the foundation for the ISF Cyber-resilience Framework, part of the Cyber Security Strategies report. By taking a broader view of cyberspace and cyber-security, senior business managers, information security professionals and their organisations will be better able to understand the true nature of the threats, in the context of the business opportunity, and respond accordingly.

About the author

Michael de Crespigny is CEO of the Information Security Forum (ISF – www.securityforum.org), an independent, not-for-profit association of organisations from around the world. His mission is to help business leaders understand what they need to do from an information security perspective to keep their businesses safe and in doing so help them succeed and protect their reputation, bottom line and share price. Prior to joining the ISF, he was a partner with services consulting firm PwC. He joined the ISF in January 2010 as COO/CFO. In addition, de Crespigny is a Fellow of the Australian Institute of Chartered Accountants and a member of the Institute of Chartered Accountants in England and Wales.

References

1. 'Cyber Security Strategies: achieving cyber-resilience'. Information Security Forum. https://store.securityforum.org/shop/cyber-security-strategies-achieving-cyber-resilience/p – 134/.

Taking the management pain out of Active Directory

Colin Tankard

Colin Tankard, Digital Pathways

Active Directory (AD) is a directory service that automates network management of user data, security and distributed resources. It is a core component of Microsoft's Windows server infrastructure and has been designed to provide a secure environment for managing users, services and resources. Its main purpose is to provide centralised authentication and authorisation for services such as email, collaboration tools, databases, applications and file shares across Windows domains. As such, it is considered to be a mission-critical part of the network infrastructure and is crucial for the internal security of the network through its ability to mitigate internal threats. But it's not the easiest system to use, which can undermine its security benefits.

However, many consider the administration tools provided in AD to be not only overly complex, but difficult and time-consuming to manage – especially as IT networks expand – and the system is also considered to be error prone, which can introduce security vulnerabilities. According to the 2011 strategic security survey undertaken by InformationWeek Analytics, 55% of organisations cite the management of complexity as being the biggest information and network security challenge that they face.[1]

The following are considered to be among the most challenging administrative tasks when using native AD tools:

- Group policy management: according to Osterman Research, 42% of users in the average organisation are on the wrong distribution lists or in the wrong groups.
- Auditing and reporting: hinders efforts to achieve compliance objectives.
- User provisioning, re-provisioning and de-provisioning: the average organisation experiences 20% internal turnover per year owing to job changes and 5% external turnover as employees leave.
- Secure delegation of user privilege: allowing business users to make