The value of a resilient cyber defence architecture

Introduction to the Cybersecurity Innovation Series

Creating and maintaining a resilient cybersecurity architecture – an architecture that is responsive to continual business change, the demands of evolving compliance and a sophisticated and hostile threat landscape – allows organisations to take advantage of new opportunities without compromise.

No business can afford to stand still and effective cybersecurity is no different. Understanding new approaches and evaluating, implementing and maintaining the latest innovative technology solutions can be difficult, time consuming and expensive.

Use the papers in our Cybersecurity Innovation Series to guide you through the latest advances in cyber approaches and technology, to focus your investments and build capability in the right areas for your business.

How to focus investment on continuous cyber confidence and capability?

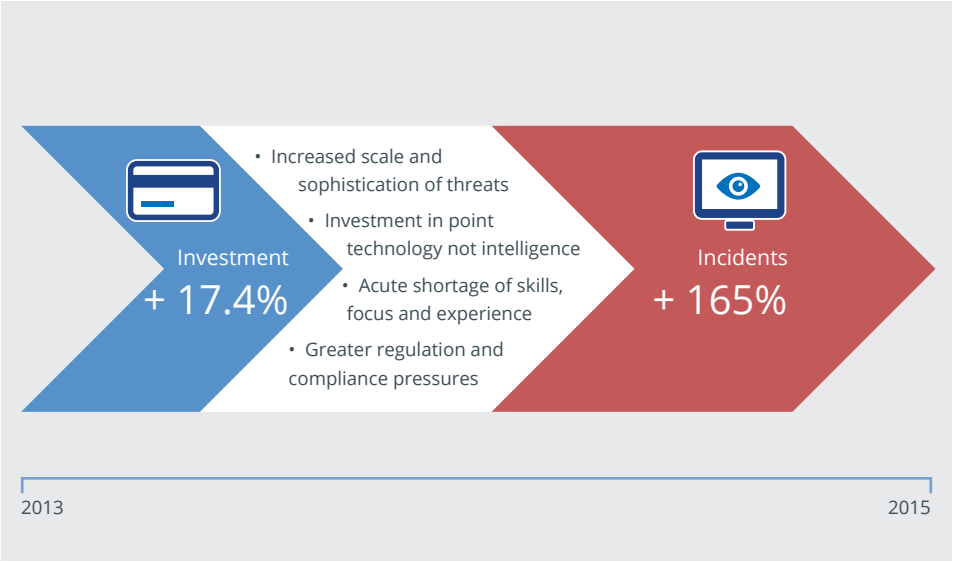
How much will your organisation spend on its cybersecurity in 2016? Is it more than last year? And if so, do you feel confident that this additional investment will deliver greater business value, in terms of risk management, predictive threat intelligence, active incident response and compliance?

If the answer to this last question is no – you are not alone. Too many organisations are spending more without experiencing the benefits of increased cyber confidence or capability. Organisations of all sizes and types feel burdened with inflexible information security architectures that are suffering from the law of diminishing returns – with budgets sucked up supporting a sprawl of technologies[1] that do not continuously increase the maturity and consequently, the business value, of their cyber response.

Research shows that, in the last two years, although worldwide investment in cybersecurity grew by 17.4 percent incidents increased by 165 percent over the same period.[2] At the same time, protecting business also got a great deal harder as specialist operational and analytical cybersecurity skills became more difficult to find and compliance and regulatory requirements got tougher.

Global business cannot spend its way out of cyber risk and increase long term capability without a fundamental change in approach. Innovation in cybersecurity need not start with a technology shopping list.

Figure 1 Security incidents continue to outstrip investment, creating a cyber intelligence gap



1. 2015 Global Information Security Workforce Study, Frost Sullivan 2. *© ISACA/RSA State of Cybersecurity survey and Gartner press release*

Information security professionals are starting to think differently about how to achieve the best cost v risk benefit for their organisations. Focusing on a core architecture that delivers a shift in continuous performance improvement, high-performing businesses are working to better align the way they predict, prevent, detect and respond to threats and breaches.

The next step in cyber maturity – building a resilient cyber defence architecture

Most businesses are striving for continuous performance improvement in everything they do. To achieve the agreed business strategy, they establish short, medium and long-term objectives and then monitor progress and performance against these metrics. Yet, rather than seeing continuous performance improvement, many organisations are trapped in a cycle of compromise when it comes to cybersecurity. Despite having a clear security strategy and policies and having invested in technology that has taken them from passive threat response to a more active approach, perhaps having even developed a dedicated security operations function, they remain unable to drive continuous performance improvement. Why?

1. **The challenge: aligning business and security strategies**

   Without executive awareness and engagement in structured, regular and ongoing conversations about risk – it remains difficult to align and adapt information security decisions with business objectives. Focused investment in what really matters to each business is the only way forward for effective cybersecurity. Organisations that are joined up in agreeing strategic priorities and performance measures elevate the conversation about cyber risk from an appeal for technology budget to an informed, fact-based business discussion with stakeholders taking part in strategic decision making.

2. **The challenge: setting long-term goals and objectives**

   Security architectures have traditionally evolved piecemeal, reacting to the evolving threat landscape or compliance requirements. The result is disparate technologies that do not continuously adapt to new threats or integrate innovative approaches to take corrective action. Data overload that hampers visibility and analysis is also a challenge to focused, agile response and future decision making. In our experience, many organisations do not maximise the functionality of their technology assets. Whether due to lack of resources or technical know-how, all too often this leads to duplicated investment or missed opportunities to increase capability.

3. **The challenge: monitoring performance against metrics**

   Security professionals have lacked the external insight and benchmarking vital to continuous performance improvement. As well as setting meaningful metrics against which business stakeholders can measure performance, organisations need to establish how their cyber capability stacks up within their industry and beyond – giving them a baseline for strategic investment and improvement. Resourcing constraints also mean that security specialists are torn between strategic and tactical activities. Unsurprisingly, team members find it difficult to move easily between the conflicting roles of predictive analyst and performing the core tactical, compliance and operational aspects of the security lifecycle.

But some organisations have overcome these challenges – bringing people, process and technology together within a resilient cyber defence architecture that is not only transforming their cyber capability and confidence, but demonstrating clear value to the business too.

So what is different about a resilient cyber defence architecture and how can organisations, already strained to the limit in terms of resources and maintaining business as usual make this transformation?

Example Case Study: Large Energy Company – Future-proofing the business with advanced cyber capability

Challenge:

The client was deeply concerned over the potential commercial impact of security breaches as it had limited visibility to pinpoint these and lacked the right resources to resolve incidents fast enough in a sea of data and complex systems.

Solution:

- Delivered a transformation programme of systems, processes and procedures to proactively manage future risks
- Specialist knowledge transfer, helping build security awareness internally
- Investment in managed services to reduce costs and drive overall efficiency

Business value of the solution:

Creating a dedicated Security Operations Centre (SOC) gave the customer a central point for efficiently handling all security issues. This visibility across the organisation meant the client could clearly demonstrate ROI and match technical deliverables to commercial goals.

Focus on capability to predict, prevent, defend and respond

The integration imperative

With its promise of a comprehensive set of integrated applications across the business value chain purchased from and supported by a single vendor, there is a reason why Enterprise Resource Planning (ERP) systems became so popular across business of all sizes.

The goal was to provide users with 'one version of the truth' to help them collaborate and make consistent business decisions. Unlike ERP, information security professionals and procurement officers are still faced with a confused landscape of point solutions – where functionality is perhaps misunderstood, under-utilised or potentially duplicated.

But having a central, consistent contextual view of cyber risk is possible. Organisations are now evaluating technology based not only its functionality, but also its integration with existing assets including Security Information and Event Management (SIEM) solutions, Security Operations Centres (SOCs) and Managed Security Services. In all cases, purchasers also need to assess how investment will enhance their existing cyber capability – to predict, prevent, detect and respond to attacks.

So how can an organisation start to construct a resilient cyber defence architecture?

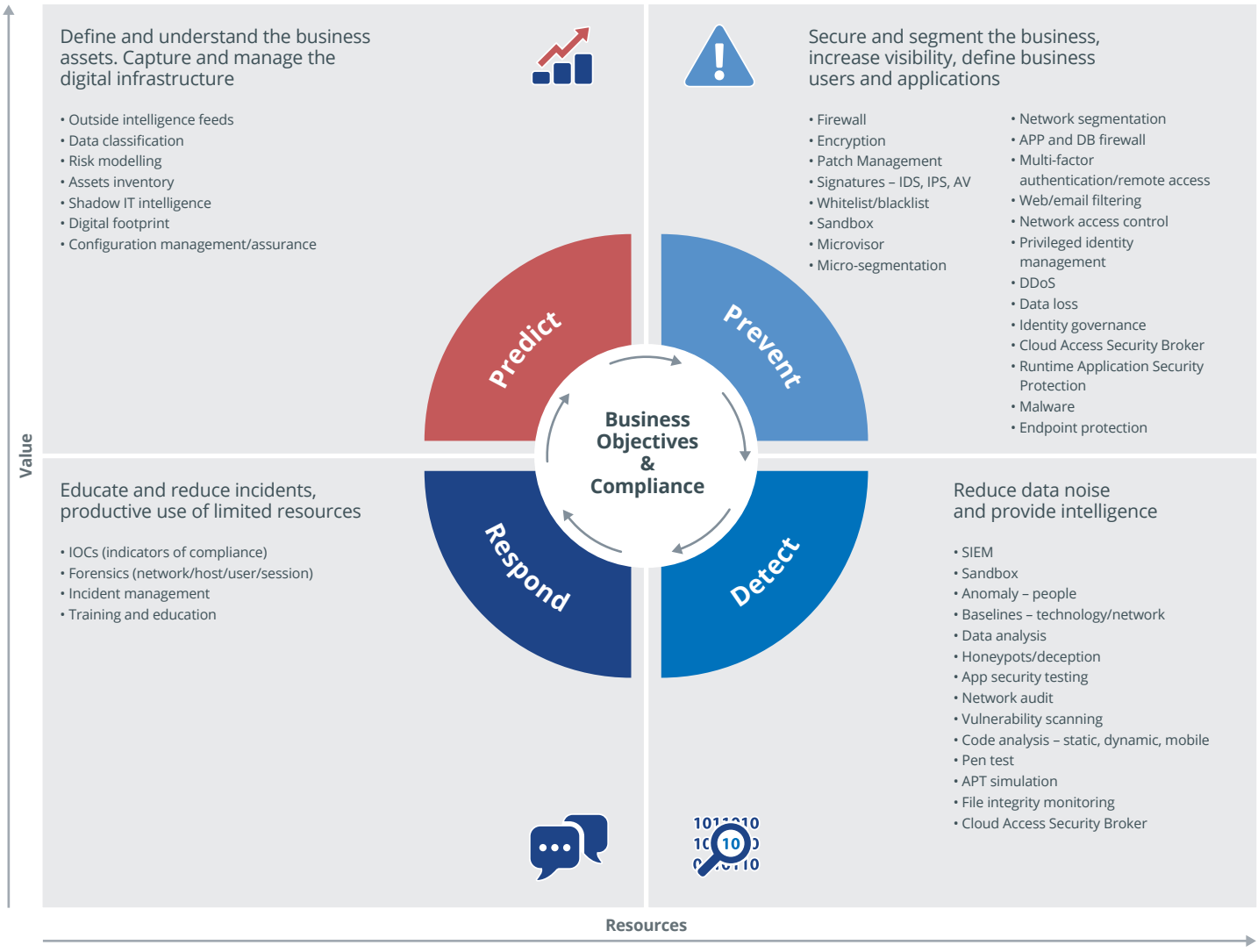
Figure 2 The security product landscape is vast, complex and dynamic. This does not mean that new and innovative technology will not continually emerge to make our tasks easier and faster, but more rigor must be applied to investment decisions.

Source © Momentum Partners, Cyber Security Market Review[3]

3. © Momentum Partners – Cybersecurity Market Review, Q4 2015 Year End

Brutal Focus on existing and target capabilities

Figure 3 Target capabilities: aligning people, process and technology to build a resilient cyber defence architecture in line with business objectives



Five steps towards a resilient cyber defence capability

For organisations that want to change their approach to cybersecurity, achieving a resilient cyber defence capability can appear a long and difficult journey – especially while they are expected to maintain business as usual. There are five steps organisations can take to make this transition, right through from scoping and evaluation to delivery:

1. Establish a resilient cyber defence architecture in line with business objectives
2. Engage all relevant stakeholders to agree performance metrics and analytics
3. Review existing technology investments against resilient cyber defence capability to identify areas of little, low or over investment
4. Review existing security teams against the capability areas to understand where your skill sets need investment
5. Create processes that ensure information and intelligence sharing between all aspects of the model and regular governance and review points to drive continuous improvement

What is resilient cyber intelligence capability?

At NTT Security, we work in partnership with our clients to build resilient cybersecurity architectures, transforming a mass of point technology solutions into a sustainable cyber defence capability. Internal and external threat data sources are transformed into intelligence that can help predict and prevent future attacks, defending the business from and responding to, current threats.

Technology innovation is at the heart of the cybersecurity industry as it attempts to keep pace with those that wish to disrupt, defraud or damage our organisations. Our technology partners consistently develop solutions that make the tasks associated with cybersecurity easier and faster – but more strategic planning, business context and rigorous evaluation must be applied to investment decisions.

This is the first in a series of four papers. Look out for the rest of our Cybersecurity Innovation series, which examines how new solutions and approaches can help to create sustainable, resilient cyber architectures - or contact us to explore how our range of innovative services can help your organisation to drive greater business value from people, processes and technology to close the cyber intelligence gap.

Our range of consulting, managed security and technology services to help our customer build a resilient cyber defence architecture include:

- Assessment services including architecture, risk, capability and compliance
- Independent technology evaluations
- End-to-end implementation experience
- Managed services to build capability such as 24/7/365 monitoring and intelligence analysis

Visit **www.nttsecurity.com** to find out more

To learn more about NTT Security and our unique services for information security and risk management, please speak to your account representative or visit: **www.nttsecurity.com** for regional contact information.

About NTT Security

NTT Security seamlessly delivers cyber resilience by enabling organisations to build high-performing and effective security and risk management programmes, with controls that enable the increasingly connected world and digital economy to overcome constantly changing security challenges. Through the Full Security Life Cycle, we ensure that scarce resources are used effectively by providing the right mix of integrated consulting, managed, cloud, and hybrid services – delivered by local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest information and communications technology (ICT) companies in the world. For more information, visit **www.nttsecurity.com**