Converging electronic and cyber security

Why you can't wait and tips for success.

Executive summary

As everything becomes more connected, so too must security management. That's the simple truth in today's increasingly complex threat environment.

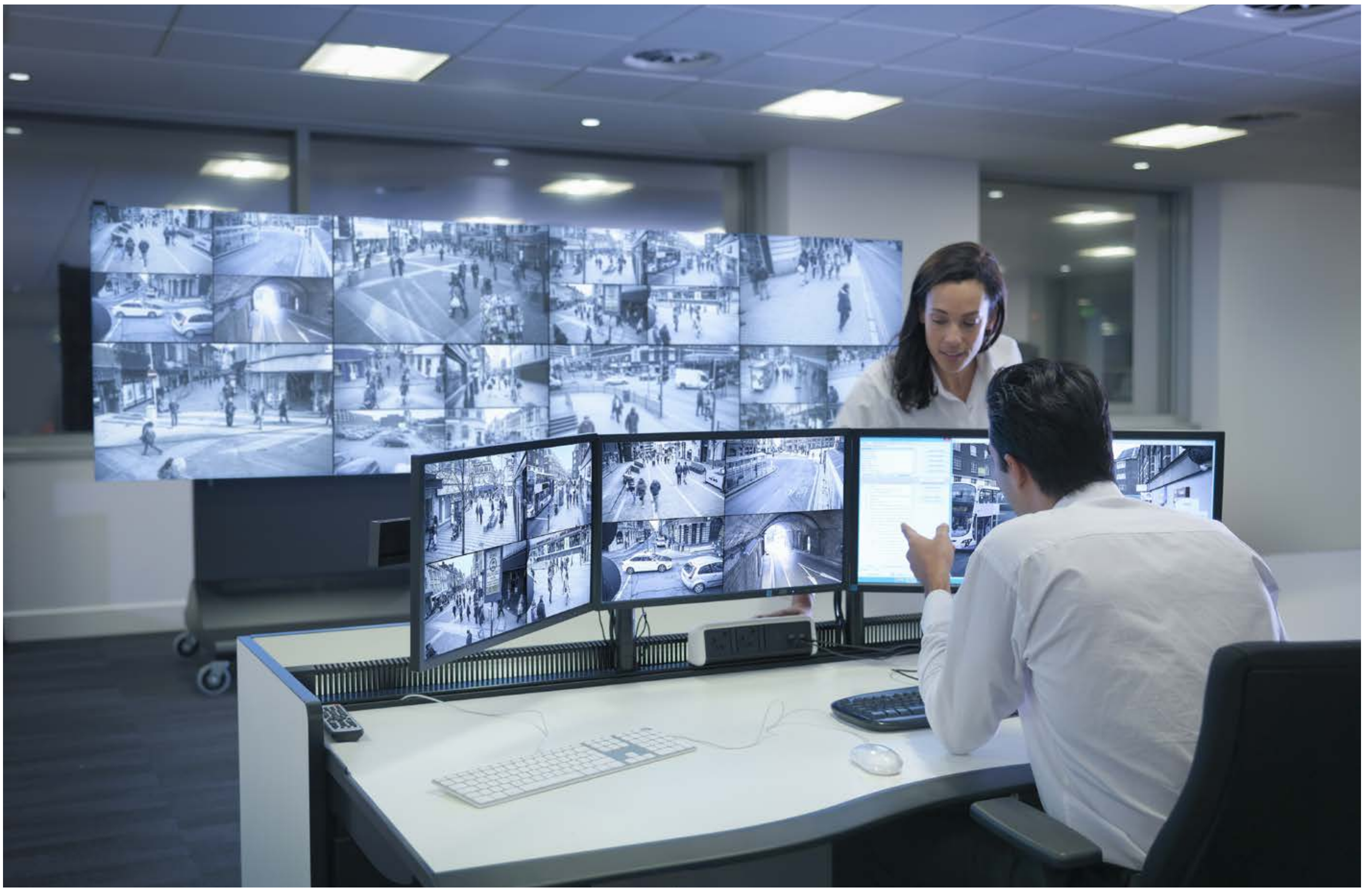
The march towards a connected future seems unstoppable. We've seen information and applications spread out to the cloud and multiple locations across the globe. Employees today are linked to each other and broader society as never before, mingling both their business and personal lives. More remarkable still is the booming inter-connectedness of everyday devices driven by the Internet of Things (IoT). All this means that traditional corporate boundaries are blurring and becoming more vulnerable.

Every business is aware of escalating risks. And all have protective measures in place. The question many are asking is what to do next. That's a good question, because one point is certain: while threats are evolving, you can't afford to stand still.

We believe the next step in managing security is to promote closer cohesion across all operations. This entails co-ordinating the usually separate functions of cyber security and electronic security. By cyber security, we mean the network and everything connected to it like endpoints and mobile devices. Electronic security refers to activities like physical access control, remote monitoring of alarms and video surveillance, and includes traditional physical security elements. Cyber and electronic security have already converged in the technical sphere. Now, it's time to bring them closer at the organisational level.

More than creating a neat organisational chart, this method requires disciplined co-operation and information sharing across all security teams. Importantly, it needs to be orchestrated from the top down and have support from board level executives.

The advantage of this approach is that you can link previously unrelated data to gain total contextual awareness across every facet of enterprise security. And the benefits are significant – from improved risk management and faster, more intelligent response, to more efficient use of resources and cost savings. By making enterprise security more inclusive, you can increase vigilance, while still remaining agile and competitive in your business environment. As such, security transforms from being a necessary safeguard to a key enabler of business.



Why it's time to unify security management

The transition towards IP networks and devices

At a technology level, electronic and cyber security have already started to converge. That's been driven by the widespread use of the IP protocol. Long a mainstay of data communications in the cyber security space, IP is now the main protocol for enabling electronic security. For example, surveillance cameras have transitioned from analogue devices to IP enabled devices. Similarly, alarm systems and access control systems like swipe cards have also moved over to IP.

The trend will continue as the **nbn**™ network rolls out to more places across the country. As businesses switch to IP enabled devices on the **nbn**™ network, they are upgrading their analogue security devices to digital equipment.

The growth of IP enabled devices is also accelerating at an unprecedented pace due to the massive expansion of IoT. More and more machines and devices are being connected, and not just for industrial applications like infrastructure monitoring. IoT is starting to permeate everyday life like unlocking doors, driving cars, taking phone calls and more. In fact, the possibilities are limitless.

More connections make you more vulnerable

As more devices and systems are linked to each other and to the internet, they present greater opportunities for attack. An example is the recent assault on the British National Health System, where criminals denied access to computer systems unless a ransom was paid.

However, the health system breach targeted unpatched systems, highlighting the need for organisations to ensure basic cyber security hygiene. The situation becomes even more challenging for security professionals when peripheral devices like IP surveillance cameras are compromised.

Any peripheral device connected to your corporate network can potentially be hacked and used as an attack tool. Instances of this have already garnered attention – the Mirai botnet for example. Mirai malware primarily infected consumer IoT devices like IP enabled cameras so the hacker could control them as a group, creating a botnet.

In October 2016, the Mirai botnet mounted a Distributed Denial of Service (DDoS) attack on Dyn, a major US internet service provider. By flooding the network with traffic delivered from hijacked devices, several high-profile websites were made unavailable to millions of people.

Personal devices like smart phones and swipe cards to access buildings create another way to infiltrate corporate systems. Which highlights the fact that no matter how good your cyber security, people can still be the biggest vulnerability in your defence. Anyone who gains physical access to your offices has the opportunity to use a terminal or plug in a USB key to compromise your business.

The exposure of personal devices is becoming more of a concern since identity or password theft is now much easier for criminals. Social Media is the main culprit for this trend because so much personal information is available freely online. Criminals can find out employees' workplace location, their full name and job description. They can even deduce likely passwords since many of them are still based on date of birth, personal events or names of loved ones. The growth in mobile malware is another vulnerability.

Criminals posed as technicians and used fake IDs to enter the server room of a major corporation. They then stole the servers, which happened to contain all the emails and passwords used in the business.

Employees can be used as a back door into your business, either over the network or inside your premises. The 'non-malicious insider', a person who unwittingly breaches security through mistakes or carelessness, is one scenario. The other is where employees themselves decide to damage or steal from your business. Inside threats can be just as damaging to your reputation and financial position as ones that originate outside company walls.

Why it's time to unify security management (continued)

Threats have converged, but security management hasn’t

Cyber attacks and physical intrusion into the premises are now working hand in glove. Network vulnerabilities are being exploited to commit physical crimes, and physical incursions are occurring to gather information or install malware for the purpose of cyber crime. These blended or converged threats will no doubt increase.

Because the payoff is so high, either through ransom demands or selling corporate information online, the presence of organised crime is also growing. Specialisation and innovation in the crime community continues, and criminals are becoming more persistent and effective. Today’s corporate intruders are professionals. They have the resources and know-how, and they will dedicate the time to infiltrate your systems if they think the rewards warrant it.

> “As long as organizations treat their physical and cyber domains as separate, there is little hope of securing either one.”
>
> Scott Borg, Director and Chief Economist of the U.S. Cyber Consequences Unit[1]

Unfortunately, the cohesive approach displayed by criminals is seldom matched by their security management opponents. Many organisations have one set of staff to manage electronic security for physical access to a facility, but separate personnel to control information and network security. Traditionally, these have been completely separate disciplines, with different goals, perspectives, training and executive accountability. That’s not to say that each security department isn’t doing its utmost. But co-ordination between the two disciplines has generally been nominal.

The lack of co-operation and information sharing between each department creates a major problem. For instance, if cyber security and electronic security have separate identity databases, how can they cross-reference between the two? And with the traditional emphasis on cyber security, how will a business cope with the increase in converged threats given that lack of co-operation?

Speed of response is a key issue. In security management, the value of information is directly related to timeliness. With the complexity of corporate systems today, lack of cohesion between cyber and electronic security can create a lag between when a threat occurs, to when it is identified, to when countermeasures are deployed. A window of opportunity opens up, ready to be exploited.

Many organisations can be lulled into a sense of complacency because they have the latest security products and compliance procedures in place. They think they are managing risk on an enterprise-wide basis, but their efforts are not co-ordinated . Consequently, their risk management procedures often cannot cover the bewildering range of applications, technologies and tools being used today, and the vulnerabilities they present to astute criminals.

What’s required is a more synchronised approach across both cyber and electronic security domains. If they are treated separately, the harder and more costly it will be to secure the business.

[1] 1. Why Integrate Physical and Logical Security? Cisco 2011 http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/pl-security.pdf

Towards a converged security strategy across your enterprise

From the above, we can draw the conclusion that security management is under mounting pressure. Threats are more diverse, persistent and targeted, and delivered by motivated professionals. Enterprise systems are constantly increasing in complexity. Traditional security barriers are more permeable. To mount an effective defence today requires a re-think of your approach to security from top to bottom.

Orchestrate your security posture

The most important step is to bring your security strategy and capabilities spanning departmental responsibilities, procedures and management closer together. A method that incorporates all forms of security – network, information, electronic and physical, and includes personnel safety. It should also provide a collaborative approach to security's role in business continuity, disaster recovery and risk management.

This is more than just improved coordination. Cultural change is paramount since you need to bring together separate security teams, with different priorities, perspectives and skills. Disciplined co-operation is required that involves processes, tools and defined aims.

When that is accomplished, everyone works in concert towards a common goal. The security response is more cohesive, with different teams working together in tandem. The synergies created mean that the whole does become greater than the sum of its parts. Now the enterprise can draw on the combined vigilance and experience of all security personnel. Total situational awareness is achieved so teams can quickly identify potential gaps, and react faster to vulnerabilities.

Critical to this approach is enabling senior security executives to have access to the highest levels of management. These executives should be able to articulate concerns to the C-suite to create an enterprise-wide security perspective that can be factored in to broader business strategies.

> By 2020 a holistic security system, encompassing every facet of the work place, will be in operation. At each level, depending on the sensitivity of the area, the security verification process will become more stringent, with the need for Automatic Identification & Data Capture anticipated to increase exponentially.[2]

Take advantage of new capabilities

While increasing inter-connectedness has created new vulnerabilities, it's also providing better ways to monitor security through new tools and deeper data.

With IoT, you can connect more types of devices more easily. These devices are being used across the wider organisation such as marketing, operations and HR. Moreover, the sophistication of surveillance, access and intrusion devices is increasing all the time. And they all provide rich data streams in real, or near-real time to improve business intelligence. The integration of structured and unstructured data sets is a case in point.

Security tools in broad use today primarily use structured or partly structured machine-generated information such as system log and network events. The most advanced of these apply sophisticated machine learning techniques to identify anomalous events or patterns. There are even tools that search natural language such as text or transcribed speech for particular content. However, a large proportion of the world's information is unstructured, such as images and video.

The new generation of tools now augment existing analysis of structured data with an understanding of unstructured data. By correlating the two, you create a broader context of threat information to help decision makers respond to an event.

> Combining structured and unstructured data can create a layered defence when used with multi-factor authentication. Licence plate recognition and video surveillance can be integrated with building/floor access cards, network log-ins and biometric scans. Security can check if users are who they're supposed to be, and where they should or shouldn't be – all from one integrated database.

At Telstra, we're moving to synchronise security services for our customers

As a large telecommunications company with multiple offices, employees and an Australia-wide presence, we understand the security problems mid to large scale organisations encounter. Indeed, we face them ourselves. So we have taken action to help our customers combat the growing incidence of threats in an ever more complex cyber and electronic environment.

Our product development teams for electronic and cyber security now work together as one, and are responsible to a single high-level executive with access to Telstra senior management. In addition, we've embraced the opportunities that new technologies can deliver.

[2] Physical Security Products & Services Market Study. Frost & Sullivan 2015

Towards a converged security strategy across your enterprise (continued)

Key among these is the Telstra Managed Security Services (MSS) platform in the Telstra Security Operation Centres. Built on open source technology, the MSS platform helps our customers manage risk and focus on security priorities. Cloud-based analytics, machine learning and rapid scalability enables fast, context-aware alert and triage. Most importantly, a single source of intelligence now underpins all of our security activities:

- Identity and Access Management – Manage access to both physical locations and digital systems
- End-Point – Secure end-points like servers, desktops and mobiles connected to the network
- Network – Protect physical, virtual or hybrid network security infrastructure, such as firewalls, content filtering and Denial of Service protection
- Cloud – Secure cloud platforms, applications and data
- Applications and data – Protect data transmitted, stored and used by applications
- Electronic – Correlation with on-premises security like video monitoring and building alarms
- IoT – Enable visibility and protection of systems of connected objects.

The Telstra OpenMSS platform is not only a lynchpin of our own security efforts, it is also available to our customers. It can be implemented in as little as 24 hours, allows you to see what we see, and offers the flexibility to only use the tools relevant to your business environment.

The benefits of converged security are real and measurable

A collaborative approach to security offers advantages at both strategic and tactical levels.

Effectiveness

An enterprise-wide perspective on managing risk – not just threats but business continuity and disaster recovery – can provide better situational awareness for event management and investigation. You can prioritise vulnerabilities and make a comprehensive, integrated security plan that considers where both the organisation and technology is going. And since security is woven into the fabric of operations, it can now align closely with corporate goals and deliver more value to business.

Responsiveness

Closer teamwork will help break down the walls between staff who previously focused on their individual security function. As collaboration among different security functions increase, teams become more aware and capable. Cross-training will also make staff understand areas that weren't previously part of their jobs. Ultimately, they're able to respond faster and more intelligently to risk. Loss and fraud prevention, employee terminations and new hires, business continuity planning, compliance and insurance can all benefit.

Efficiency

Tighter integration can deliver the same advantages to security as with any other part of your business. Moving towards common infrastructure across departments, reduced cabling, a single control platform and a single operating system can trim management, maintenance and costs. Staffing resources can also be employed more proficiently as you reduce inter-departmental inefficiencies.

Approaching security convergence

The first step in approaching convergence is to understand where you are so you can determine where you need to go. At Telstra, we use a framework to present security so everyone can engage. It allows senior executives to contribute to managing risk and involves staff members at all levels. The framework understands that security is a human issue as well as a technical one, and provides an enterprise-wide focus. We call it The Five Knows of Cyber Security, and we believe it is the first step in creating a solid security foundation.

Know the value of your data.

All data has value to someone. You need to know what value it has, not just for your organisation and customers, but also the value to those who may wish to steal it.

Know who has access to your data.

Who has access both within your organisation and externally? Who has 'super user' admin rights in your organisation and within your trusted partners and vendors?

Know where your data is.

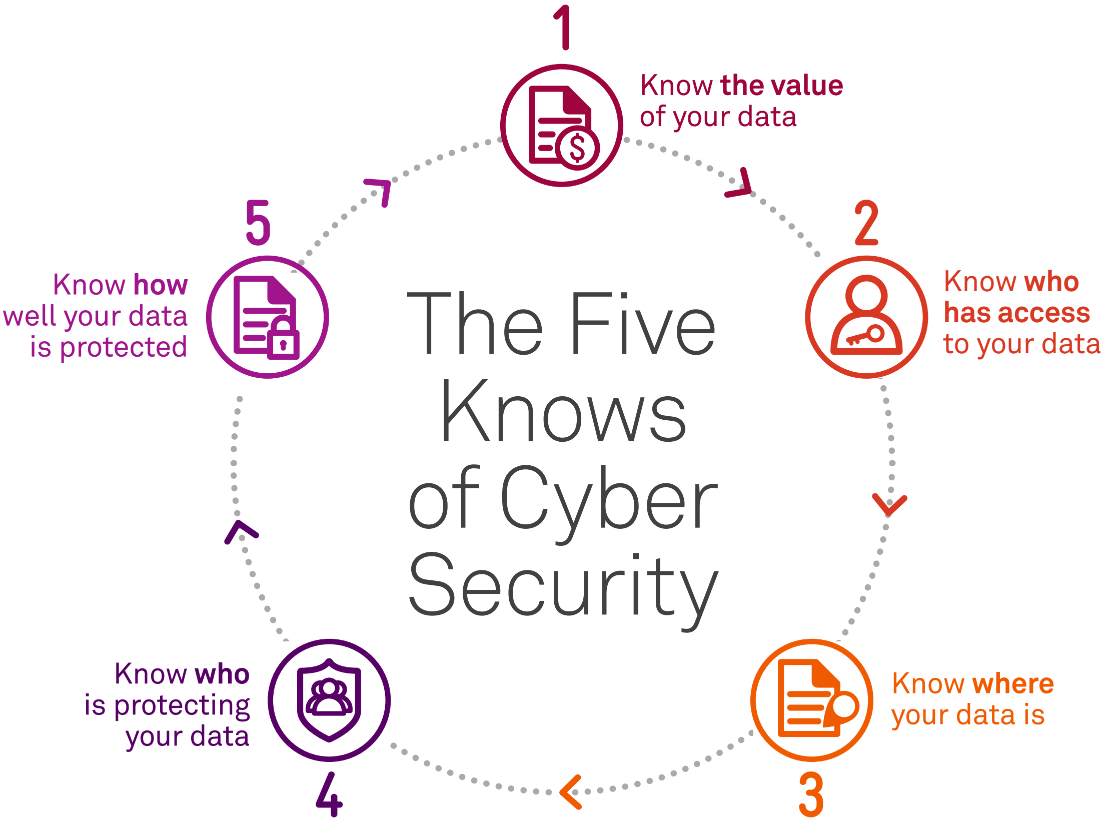
Where is your data stored? Is it with a service provider? Have they provided your data to other third parties? Is it onshore, off-shore or in the cloud?

Know who is protecting your data.

Who is responsible for protecting your data? Where are they, and can you contact them if you need to? What operational security processes are in place?

Know how well your data is protected.

Do you know what your security professionals are doing to protect your data 24/7? Is your data being adequately protected by your employees, business partners and third party vendors who have access to it?



The Five Knows of Cyber Security

1
Know the value of your data
2
Know who has access to your data
3
Know where your data is
4
Know who is protecting your data
5
Know how well your data is protected

Approaching security convergence (continued)

Assess your readiness

When moving towards a more orchestrated security posture, six key factors need to be examined to ensure that both cyber and electronic security teams are ready:

Business.
What business problems are you solving? What value will convergence bring to your organisation?

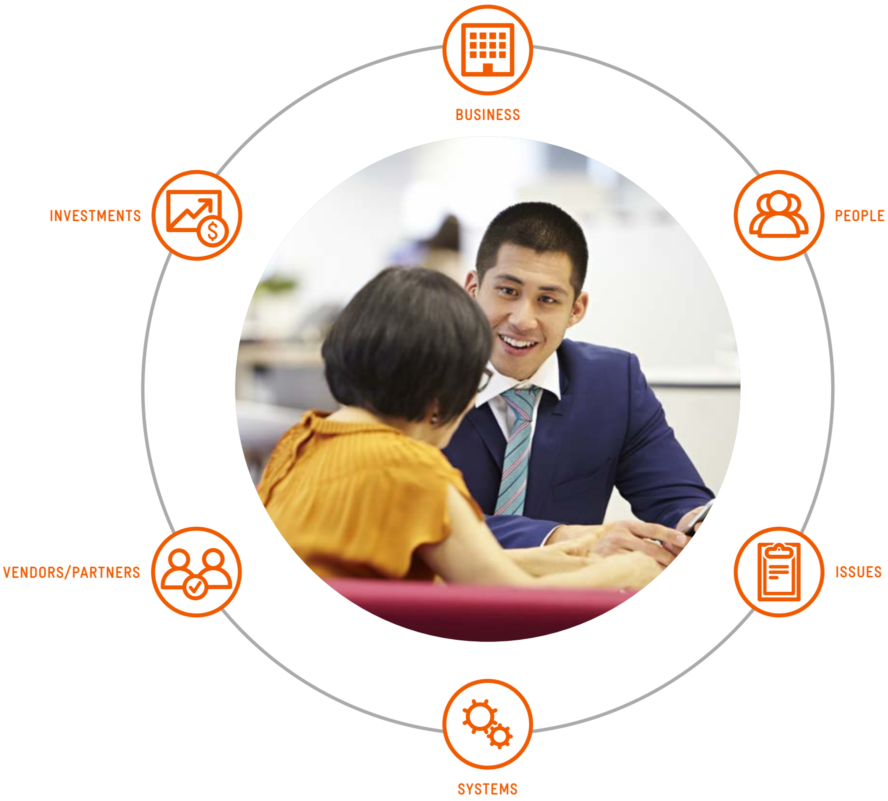
People.
Do you know which owners, decision makers and departments are involved? Can you get executive sponsorship?

Issues.
What will the converged structure look like – will there be formal or informal co-operation? How will you manage cultural differences among staff, whose backgrounds span network, server, and software security to police work, fraud investigation and intelligence?

Systems.
What are you trying to protect? What systems and information do you already have, and what do you need in the future?

Vendors/Partners.
Are your suppliers reputable? Do they understand different types of security requirements? Do they have appropriate security controls (e.g. patching) in place? Do they regularly communicate known issues and updates?

Investment.
What is your risk profile, level of required integration and deployment timeframe? What is your investment roadmap over the short and longer term?



Next steps

With the increasing diffusion of corporate boundaries and growing threat complexity, we believe that security convergence in the enterprise is a matter of when, not if. Investigating your options sooner rather than later is the smart move.

The good news is that you don't have to make the change in one dramatic shift. You can start by ensuring that there is a shared vision across your electronic and cyber security groups. As each group invests in infrastructure and develops processes and capabilities, it is done with interoperability, and ultimately convergence, in mind.

If you would like advice on how to approach convergence, we are qualified to help. We not only draw on lessons learned from our own journey, we offer practical insight from helping customers manage risk and protect data for decades. More than that, we can provide fully integrated solutions across secure communications, electronic security and cyber security.

About the author

Neil Campbell
Director, Global Security Solutions, Telstra

As Director of Global Security Solutions at Telstra, Neil Campbell is responsible for driving Telstra's security strategy across all of the markets that Telstra operates in around the world. Having spent more than 25 years specialising in cyber security, Neil's diverse experience includes running both boutique and big four consulting teams, and nine years in the Australian Federal Police with most of his police service in the AFP's Computer Crime Team.

contact your Telstra account executive
call 1300TELSTRA (1300 835 787)
telstra.com/enterprisesecurity