COMPETING FOR CUSTOMER SECURITY

Supporting Enterprise Security Risk Management:

How vendors can support ESRM and CSM strategies

AXIS COMMUNICATIONS

Virtually Informed
informing decisions - leading action

Unified Security

Foreword
from our sponsors

Effective cyber security is about assessing risks and consequences and taking appropriate steps. It's about products, people, technology and ongoing processes, and about partnering with a supplier that's prepared to support you at every level. Which is where Axis enters the picture.

At Axis we are proud of our 30 year unwavering support to our partners and we believe that our 100% focus on cyber security makes us the perfect partner for cyber protection. We are delighted to have commissioned and sponsored this document from Unified Security Ltd' research. We believe its recommendations for our partners and customers operating in the Enterprise Security Risk Management space will be invaluable.

In addition to this report there are a number of Axis documents and educational items available on the subject of cyber security. You can visit our Cyber Security portal at: www.axis.com/global/en/about-axis/cybersecurity to find out more. We strongly recommend all of our customers visit the portal and download a copy of the Axis Hardening guide which offers practical advice to protect your security solution.

Steven Kenny
Business Development Manager
Axis Communications

"Concern about cyber crime via IP camera networks is real. And there's no magic bullet – no single solution for staying safe."

Contents

Foreword from our sponsors	2
Executive Summary	4
Introduction – What's changed?	6
Responses to change	11
Stakeholders needs	15
Converged Security Management Requirements	20
Vendor Support	24
Author Biographies	27

Executive Summary

The background to this paper is effective Enterprise Security Risk Management (ESRM), and in particular the issue of buying and selling by and to, siloed physical and logical security teams.

The siloed approach has worked to some extent for decades, although it is questionable whether it is still working for today's complex world or enterprises.

In the same way that effective and successful incident response management necessitates actions and activities at a strategic level involving all relevant functions, through to rigorously testing plans, so too does effective and successful ESRM. It includes utilising an approach which brings together both physical and logical security professionals and teams. This multi-disciplinary approach is often called Converged Security Management (CSM), and it gets beyond the silos that have traditionally restricted a single view of Security Risks.

One of the key stumbling blocks to CSM is the use, ownership, and security of the different devices and systems used by physical security teams which are used to silo the various security teams. This came to the forefront in September 2016 when CCTVs and DVRs were used to launch a Denial of Service attack against the Internet infrastructure.

Enterprises' security teams asked themselves if their "CCTV and DVRs were vulnerable to be used as weapons to attack others"? This, in turn, raised many other questions about the security of devices used by physical security services. These questions and issues have been considered long before 2016, especially by supporters of CSM.

This paper is an attempt to collate changes which have led to this important turning point for many security teams to take action, and what stakeholders need to do to support a converged buying security team.

A converged buying security team implies a single vision and set of requirements where the devices / systems are secure having been designed, developed, and supported for security throughout their lifespan. The authors provide two distinct areas for physical security vendors to demonstrate their ability to provide solutions for enterprise security risk management rather than just surveillance systems for physical security teams.

The first is in product information and support to stakeholders throughout the lifespan of the products and involves ensuring clear messaging on the security of the devices / systems and their contributions to the overall solution of ESRM. The work in this area is mainly within the distribution and installation networks.

The second area is the security of the product itself, and includes how the vendor has matured in instilling secure by design principles through to how it deals with vulnerabilities once devices / systems have been installed at customer sites.

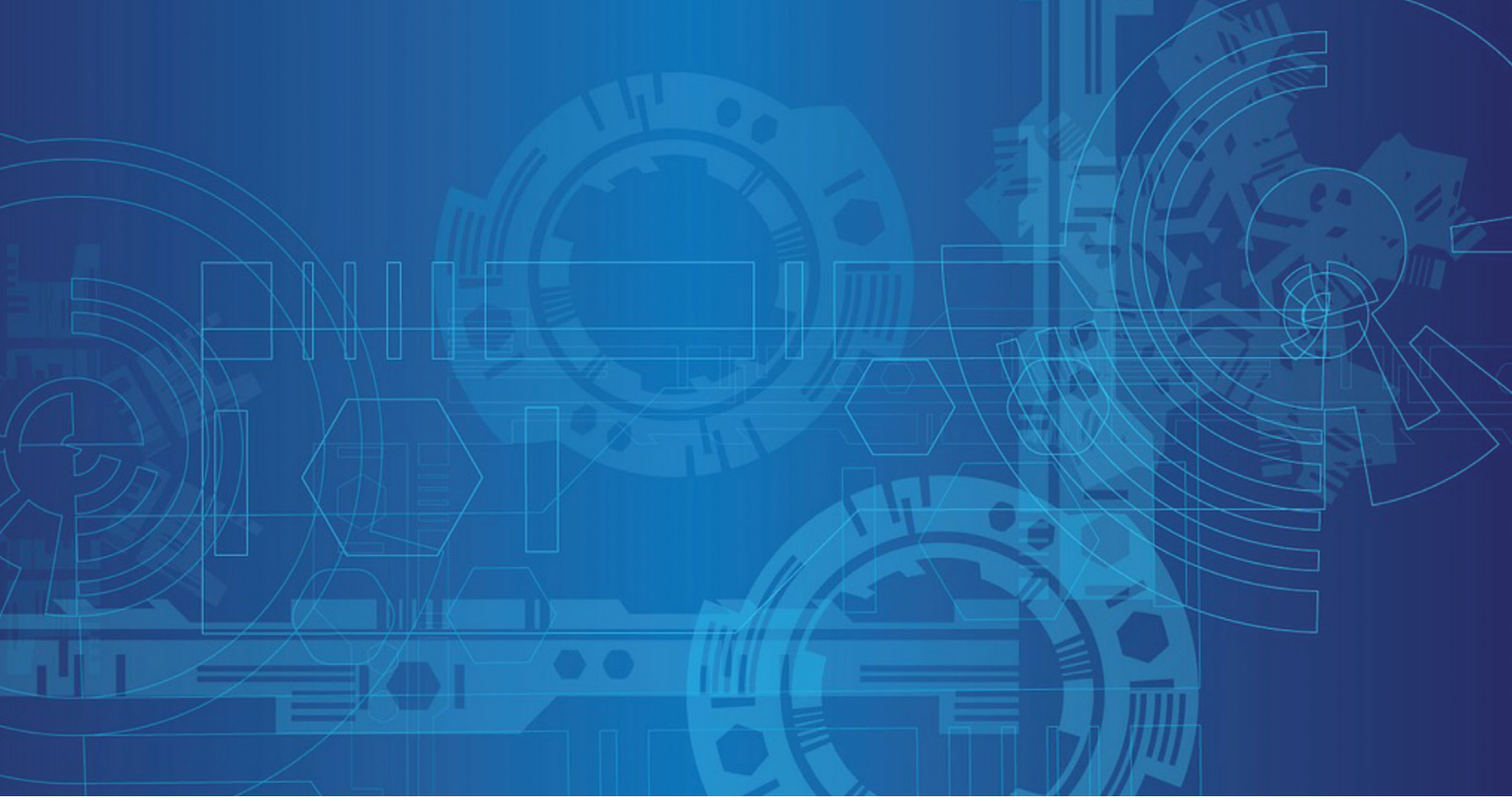
Both areas require a combined response to be able to truly offer enterprises the ability to identify threats and manage risks effectively. Jointly, these areas may be considered as the last external pieces of the CSM jigsaw puzzle. By acting on these areas, physical security vendors will be able to not only level the playing field compared with logical security vendors, but in some cases overtake them in terms of maturity in integration. The authors believe that a CSM approach to security management helps safeguard all organisations in the fast-changing world we live in. The principles outlined in this Paper could be an invaluable resource for proponents of ESRM and CSM as they develop their security strategy to manage complex risks with converged technologies.

These technologies will increasingly be deployed in SMART cities, and security professionals will need to be agile enough to respond quickly to blended security risks to the cyber physical systems on which they rely.

"...a CSM approach to security management helps safeguard all organisations in the fast-changing world we live in."

Finally, we would like to acknowledge the support of Axis as sponsors of this Paper. We welcome their interest in converged security risk management but also the work they have undertaken internally to achieve some of the changes proposed here. We would particularly like to thank the cyber security team leading the changes within Axis for recognising that the issues raised in this Paper are not just for CCTV manufacturers but all security hardware manufacturers, as well as all security teams and not just physical security teams.

We hope that security hardware manufacturers and security teams everywhere will find something of interest to work on. For that reason we intentionally kept the discussion at a very high level, with the aim that it will introduce the issue now, and that the finer details can be produced at a later stage.



Introduction
What's changed?

Converged Security Management (CSM) is a multi-disciplinary security teaming approach, which identifies and responds to the cyber-physical security risks faced by an organisation.

Cyber-physical systems now also contain physical security devices such as IP cameras and access control systems as they connect to the Internet. CSM is increasingly being seen as an effective strategy to manage these complex risks. Vendors in the physical and logical security markets are responding with more sophisticated technologies which recognise and reduce these risks by providing better intelligence for risk decision making.

This Paper will consider the role of key stakeholders in providing enterprise security risk management solutions including the Original Equipment Manufacturer (OEM), the buyer and the end user. It discusses the importance of all third party suppliers and the security of the components they provide. It will also outline the principles of Converged Security Management and indicate how lessons from leading authorities support a multi-disciplinary teaming response to security risks.

Traditionally, vendors of physical security products have sold to physical security managers, and logical security product vendors have sold to logical security managers, with each one operating in their own silo. For many enterprises, those days are gone.

In the past physical security OEMs have mainly sold 'surveillance products' to physical security

managers with a background in the police or military services. Today, they are more likely to be seen as selling 'security tools' to enterprise security teams with a requirement for a surveillance tool to integrate into the rest of the 'best of breed' products for managing their security risk programme.

In this Paper, the authors seek to:

- Provide buyers with a list of considerations for identifying innovative physical security vendors which have a strategic understanding of providing integrated enterprise security tools that meet more than just basic surveillance requirements
- Provide physical security vendors with some considerations of enterprise security buyers.

This Paper begins with an exploration of some of the changes which have brought about the necessity to adapt. Then, it considers the impact of these changes, before going on to discuss the various needs of the many stakeholders including the end customer's security management priorities. CSM and its benefits for enterprise security teams are then considered with the paper concluding on how physical security vendors can respond to meet the needs of the enterprise.

The remainder of this chapter identifies some of the contributing changes necessitating a different approach.

Governments and Regulators

Changes from governments and regulators have been subtle yet vast around the world. Here are the key changes:

- The last time the WEF commented on 'convergence' was in its Annual Global Risk Report 2016, when it stated, "While there are many "C" level owners (CISO, CFO, CEO, CRO, Risk Management), each of these owners has differing but related interests and unfortunately often does not integrate risk or effectively collaborate on its management" (WEF, 2016, p 78).
- Most governments around the world have created a cyber security strategy, recognising and accepting that the economy and democracy rely on implementing an effective cyber security strategy
- Various EU initiatives have focused on security, surveillance, and privacy, including a) The EU NIS Directive article 50 calls on manufacturers to enhance the security of the Network, b) EU Data Protection Directive (Directive 95/46/EC) is based on principles, one of which is 'Security', once collected, personal data should be kept safe and secure from potential abuse, theft, or loss. This is extended in the more recent EU GDPR. c) The EU GDPR impacts users and suppliers of services around the world.
- Since the Snowden revelations, there has been a recognition that citizens must be able to expect a level of privacy (especially from foreign surveillance), and yet the security services and law enforcement need to be able to protect against foreign state intervention and terrorism
- In the UK, the Government created the Cyber Essentials standard as part of its cyber security strategy to ensure that local SMEs are able to provide security assurance.

Usually governments and regulators only respond as a last resort; many around the world have accepted that cyber security is vital to maintaining the continuity of a country's economy and national security.

1. World Economic Forum (2016): The Global Risks Report 2016; http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf; accessed 29/05/2017.

"...there are still no standards for very basic security of an IoT device."

Standards and Frameworks

The number of security standards and frameworks has grown yearly, and is often led by industry leaders with the view to raising the bar to entry. The key changes related to standards and frameworks include:

- A continued maturity and refinement of existing enterprise information security standards and frameworks (including ISO, NIST and COBIT)
- A maturity and refinement of the use of security standards for products
- The creation of new standards for:
  - organisational security standards for SMEs supplying government contracts (Cyber Essentials and NIST)
  - Product and Industry specific standards for securing (IoT) products with common components, e.g. those for cars and healthcare
  - Developing application code.

The development, growth, and maturity of thought leadership behind many of these standards would lead one to believe that the world is in a healthy state. The truth is that since a majority of OEMs are not securing their devices, those who find the situation unacceptable stand out from the majority and have led the charge for these standards. However there are still no standards for very basic security of an IoT device.

Growth of enabling technologies

Many physical security products fit into the category of IoT products, and the IoT revolution is the result of a combination of several related changes including:

- The reduction in price of components, sensors, and related services (including sensors, chips and storage).
- Global mobile phone adoption has meant people want both access and control of things from anywhere using mobile apps and are able to do so through an Internet connection.
- The rise of Application Programming Interfaces (APIs) developed to take advantage of the latest technologies (AR, VR, AI, Big Data, etc).

Although it is individual products which are categorised as IoT products, physical security services are not so easily categorised although they may rely on hardware which is.

Technology convergence and pervasiveness

The technology convergence and pervasiveness changes include:

- The availability of data networks from almost anywhere.
- Most households have at least one mobile device per individual with which they can access the Internet.
- The use of ethernet networks as a de facto connection to access, manage, and control devices and collect and manage data using mobile apps.
- New interfacing devices perform multiple tasks, and non-interfacing devices are able to collect and disseminate data to numerous collection points
- Cloud services for apps and data storage have grown for almost every conceivable use possible in both home and work lives.

The last 10 years have brought unprecedented technology convergence and pervasiveness.

Daily business threats

The threats an average business faces each day have been growing depending on the industry sector. The changes related to daily business threats include:

- New products, new code and new apps all bring vulnerabilities, which may be exploited in multiple ways, including creating new malware.
- Where there are no technical vulnerabilities, human vulnerabilities are used in the form of scams, to get users to either part with money or to compromise their devices.
- Due to password reuse practices, new breaches may mean compromises of other services.
- Staff may pose threats as malicious insiders or through accidental action.

Many of these threats often expose the lack of rigor in implementing security procedures in many organisations.

Threats to Infrastructure

Successful attacks to the Infrastructure were relatively unknown until last year especially not any initiated using physical security products. Below are the key changes related to threats to the infrastructure:

- September 2016's first ever coordinated attack using CCTV and DVR devices (https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/)
- Mirai botnet took down parts of the Internet in September 2016 (https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/)
- 120,000 IP cameras vulnerable to the Persirai botnet (http://www.zdnet.com/article/120000-iot-cameras-vulnerable-to-new-persirai-botnet-say-researchers/)

As there are so many IoT devices connected to the Internet, cybersecurity professionals are expecting that it is very likely that there will be more similar types of attack perhaps using different vulnerable end point devices.

Cyber-criminal related changes

Criminals have leveraged technology to commit cyber enabled crime over the last few years:

- Hacker business models have become highly professionalised and specialised:
  - Some offer point and click tools to quickly set up and generate revenues
  - Compromised devices are hired out by the hour
  - Some offer money back guarantees if their tools are unable to evade commercial anti-virus products.
- Hackers are taking advantage of the fact that Apps are not developed by developers who either understand secure coding practices or with security in mind
- Criminals have utilised unskilled innocent people being used as money mules to collect the money so they are not caught by law enforcement.

Many believe it is a cat and mouse game with the criminals higher up staying ahead.

Kia Controlroom.

Device related changes

The makeup of an IoT device is very different today. Here are some of the high-level changes:

- Previously physical security devices were intended to be accessed from a small number of known end points. Today's devices may be accessed over the Internet from any number of endpoints, anywhere in the world.
- Although there are many benefits for devices to operating on an IP network, there are also significant disadvantages, least of all are the numerous vulnerabilities in all the components and technologies which may be used.
- Many IoT devices are complex computers comparable to the devices any world leader would have used 10 years ago for their day to day business.
- Last year the world experienced its first DDoS attack caused by compromised IoT devices (CCTV & DVR's).

Various researches have shown that most device compromises are due to the lack of simple controls not being implemented or utilised. With so many new IoT devices connecting to the Internet via work networks, enterprises will need to be vigilant that they are not contributing to attacks originating from their networks.

Differences in logical and physical security vendor approaches

Different industries, markets, and professions work using different approaches. Below are some of the historical differences of logical and physical security vendors:

- At a very general level, logical security vendors are expected to provide products which are secure, and developed utilising secure development practices. These vendors are aware that their customers expect that security products should not be sold with vulnerabilities. For physical security product vendors, the buyers are less likely to be able to challenge the vendor about the security of its products.
- At a very general level, logical security vendors are usually selling to someone who understands application and product development, as well as vulnerability management. This has not usually been the case for physical security product vendors.
- Many logical security vendors have, for several years, had the approach of selling risk management tools to achieve regulatory compliance. Many of these vendors often partner with others to provide more comprehensive solutions than they could provide alone. Physical security product vendors were usually considered as selling surveillance products.
- Although there are no known studies comparing vulnerabilities or attacks to and from the two groups, recently there are more press-worthy reports of physical security products being compromised and utilised for denial of service attacks (using compromised CCTV and DVR as part of a botnet).
- Due to their different histories, logical security products may be seen as tools requiring many hours to configure to get the best on the network and considerably fewer hours to lock down. Whereas, some physical security products may require fewer man hours to configure but more man hours to lock down.

With the EU GDPR it is probable that most security products are going to have some compliance implications.

In summary, the vast number of changes illustrate once again that the only constant that can be relied upon is change itself. These changes present enterprises with multiple challenges.

Responses to change

The range of changes identified in the last chapter may result in specific organisational, technological and strategic responses depending on country, industry, business, board, etc.

It would be a lengthy task for the authors to explore responses to all changes, so this chapter explores some of the general impacts of some of the changes and responses.

Government and Regulators

The response by enterprises to increased regulation is often to continue their path, to either maintain their process maturity levels, or to show willing by moving up the maturity levels.

All this is usually undertaken in the name of compliance, the necessity to comply has become a goal in itself for some enterprises in the highly-regulated industries.

The critical national infrastructure organisations have had to provide greater assurance on their ability to respond to and contain incidents. Meanwhile some SMEs have very slowly been waking up to having to provide security certifications to be able to compete for government contracts. Social media businesses have either been making a stand for privacy and against government surveillance, or complying with requests for data. So far no service provider has publicly offered to provide any government back-doors into their data.

Since 2013, as a result of the rapid advances in technology and the security risks they pose, governments, businesses, security professionals and academia have called for and worked on

new cyber security strategies and frameworks. These indicate there are increasing risks from the IoT. It is perhaps the risks of physical devices and SMART Grids connecting to the Internet which has caused most concern but what is particularly significant are the findings.

There are two of particular importance for CSM.

- There is a common view expressed that until recently most risk management strategies have been siloed with Information and IT Security responsible for cyber security and Physical security the traditional attacks
- Some also recommend that an integrated security risk management and holistic approach is adopted to enable a more resilient business environment and greater security in devices.

Security Associations' collaboration and Surveys

Since the formation of the Alliance for Enterprise Security Risk Management in 2003 ASIS International, ISACA, ISSA and ISC (2) have recommended an integrated security risk management approach. In 2016 a comprehensive report by the Perpetuity Research Initiative showed that 27% of security functions operate in a single team (Gill, Howell. 2016). The ASIS/ISAF survey in 2012 found that 55% of security professionals worked together on the implementation of new IP video systems with 39% reporting in to the same risk executive (ASIS/ISAF, 2012). It is significant that in November 2016 ASIS International made Enterprise Security Risk Management a global security initiative. It is also noteworthy that ISACA and ISC[(2)] joined ASIS in April 2016 for the first time to announce the collaboration of all three global security associations to write a new Security Awareness Standard. Each of these developments demonstrates a commitment from security professionals to working together on security risks from an enterprise perspective.

Technology convergence and pervasiveness

Technology and increasingly the physical devices sold by vendors are converging on the corporate network and through personal mobile applications. Whilst the business is often enthusiastic to implement the latest technology it is not always as secure as the security team would like. It is however crucial that all new physical security systems are considered together with the organisation's cyber security team/specialist. The rapid growth in the IoT has meant, according to DHS,

"This interconnectedness of devices introduces cyber-physical technologies that connect cyber systems to physical systems, thereby removing the barrier between the cyber and physical worlds..... but the greater connectivity also expands the potential attack surface for malicious actors."[(4)]

The impact on Physical Security Vendors and Suppliers has been:

- Some physical security vendors are now addressing the potential cyber security risks of their products in a bid to compete effectively in the market place and assure the end users that they at least are reducing the risk from their side
- The more mature physical security suppliers understand the importance of compliance and risk management which logical security suppliers have identified for many years.

2. ASIS/ISAF (2012) The ASIS/ISAF Security Convergence Survey. http://www.asisonline.eu/docs/2011-12-asis-isaf-security-convegence-survey.html accessed 29/05/2017.
3: Gill, M, Howell, C (2016) Tackling Cyber crime and the role of Private Security (A Security Research Initiative) Perpetuity Research and Consultancy International (PRCI) Ltd https://perpetuityresearch.com/wp-content/uploads/2016/09/SRI-Report-2016.pdf accessed 29/05/2017.
4. DHS (2015) DHS Report on Cyber-Physical Infrastructure Risks to Smart Cities, The Future of Smart Cities: Cyber-Physical Infrastructure Risk; https://publicintelligence.net/dhs-ocia-smart-cities/; accessed 29/05/2017.

Impact on Enterprise' Security Strategy

Some businesses have responded in quite significant ways to these changes. Since early 2015 there have been notable developments, in particular, for example, in the converged security field which have affected both the end user and the vendor. Barclays and Symantec have merged their security functions. Troels Oerting, CSO of a new converged security function at Barclays stated,

"By integrating the duplicative functions, building security operations centres, and by focusing on all aspects of Security – People, Processes, Technology – companies can direct, monitor and control the implementation of Security and Trust as a whole" (Oerting & Kvochco , 2016, p 2).

Several large physical security suppliers have developed converged cyber physical technologies and partnered with cyber security companies. In part this is due to the media attention on cyber security and the growth in the number of high profile hacks on physical devices from cars to BMS and CCTV systems. This is now challenging others in the field to consider what they should do to keep pace and assure their clients that the physical systems they provide are reliable, secure and safe to use.

The BSIA, stated in September 2016: "end users of IP connected CCTV systems should also ensure that they have comprehensive cyber security and information security policies in place" (BSIA, 2016).

But we might realistically ask just how many are following this excellent advice? If the US is anything to go by then we should be concerned as the US Govt audit office found, 'no one within DHS is assessing or addressing cyber risk to building and access control systems particularly at the nearly 9,000 federal facilities' (GAO, 2015).

There has however been a good response since that report was published and it helped alert the industry to the problem. It was probably the Mirai Ddos attacks in June and September 2016 which really have forced both the end user and the vendor to address the issues they face. The malware which led to the successful attack means that there are now over 200,000 cameras that are vulnerable to further exploitation. The incident clearly prompted the BSIA to emphasise the importance of this emerging area and accelerated more companies to develop their converged approach.

This kind of strategy has an impact not only on organisations, but also on suppliers as more businesses see the value of merging their security teams under a single leader. Businesses will increasingly expect their security solutions to be reliable, safe, and robust. This is because they will want to follow advice from engineers who understand the risks of cyber physical systems and not simply those who can implement a physical security system. Why, because as was demonstrated in the introduction, physical systems are now connected to the Internet and managers are using SMART phones to monitor physical security over an Internet connection. As soon as this happens the physical security system is vulnerable to a cyber attack and there is a potential for company data to be breached.

5. Oerting & Kvochco (2016) Three Ways To Re-imagine The Role Of Global Security Teams; https://www.forbes.com/sites/elenakvochko/2016/08/08/re-imagine-global-security-teams/#5361e29e4dc5; accessed 29/05/2017.
6. BSIA (2016) Consider network security when using IP CCTV surveillance systems warn BSIA members:http://www.bsia.co.uk/LatestNews/tabid/87/ctl/NewsItem/mid/431/Id/188/Default.aspx?returnurl=%2Fdefault.aspx; accessed 29/05/2017.
7. GAO (2015) FEDERAL FACILITY CYBERSECURITY: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems: http://www.gao.gov/products/GAO-15-6; accessed 29/05/2017.

Manufacture and systems' design management

The many changes outlined in chapter 1 have also led some Manufacturers to consider the design and manufacture of the product. The following are indicators of this shift in thinking.

- NIST has indicated that a Cyber-physical system (CPS) device is, "A device such as a video camera, robot, or thermostat. The focus of the analysis would emphasise the robustness of the design to enable it to become a valued component of a CPS". (NIST, 2016, p 25)
- End users need to understand the vulnerabilities of these devices and protect them on the corporate network
- Vendors must first design and then manufacture products which consider the cyber security aspect
- In the past, this process has tended to be separated for physical systems but not in logical
- NIST Framework concludes the threat now is from a 'co-ordinated exploitation of both physical and cyber vulnerabilities' (ibid, p 52).

Enterprise' Board's main concerns

Fundamentally the main concern for enterprise' boards and end users is how physical security systems can lead to cyber security breaches which might mean they have to pay large fines when the new EU General Data Protection Regulation comes into force in May 2018. Some will think that a CCTV or access control system is not considered as a relevant threat vector by the UK Information Commissioner. They might think that the issue is mainly on the security of the images and passes alone. However there is a definite link between physical and logical systems and data in the GDPR as outlined in Article 32.

Article 32, the Security of Processing, states,

– 'the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including...

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;"

Important points to consider for security professionals:

- Most if not all Information security professionals are conscious of the importance of this new legislation; many physical security specialists are not aware of its relevance to physical security
- The mention of a 'physical' incident here ought to indicate to physical security managers and strategists that this legislation also affects them
- The organisation needs to implement technical measures to ensure a level of security to restore the systems
- The costs of a failure to do so could result in a fine of 4% of a business' annual turnover.

In the next chapter the authors will outline how technology provided by vendors and third party suppliers can be managed to support the end user and thereby demonstrate the significance of a strong partnership between them and achieve organisational resilience.

8. NIST (2016) Cyber Physical Systems Public Working Group: Cyber Physical Systems Framework, May 2016.https://pages.nist.gov/cpspwg/ accessed 29/05/2017.
9. European Union (2016) General Data Protection Regulation; http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

Stakeholders needs

To achieve the goal of changing from selling a surveillance tool to selling a risk management or compliance tool may mean that all relevant stakeholders' needs may have to be considered and streamlined for the targeted customer and users.

In this chapter, we consider some of the individual stakeholders and their needs / requirements to be able to make the shift to selling a risk management / compliance product.

The obvious key stakeholders are the Original Equipment Manufacturer (OEM), the customer who will buy the product and the end user (sometimes these are different, other times the same). Within each of these three there will be several internal stakeholders. The other stakeholders who play a role in the product ecosystem are many and varied depending on the product in question. The following page shows a graphic depicting the range of stakeholders.

Figure 1 is broken down into three sections:

- The top section of Figure 1 shows stakeholders and their level of involvement over the life cycle of a product. The different groups of stakeholders within the key stakeholder are not shown (e.g. product development, marketing, sales, audit, risk team, network team, etc.). The group of external stakeholders not contributing to the actual product are all shown in green surrounded by a broken line to indicate that their involvement, participation, responsibility and contribution may be impacted at any time over the life cycle of the product.

- The middle section identifies some of the key processes over the life cycle.
- The bottom section identifies some of the key documentation over the life cycle.

The remainder of this Chapter details the needs of the stakeholders during the lifespan of a product.

Original Equipment Manufacturer (OEM)

As the OEM, and with the most to gain from meeting any stakeholder needs, it is almost entirely up to the OEM to meet the appropriate needs of the various stakeholders in their roles in making a successful sale to a happy long term customer. Also, along with the customer, the OEM is likely to have the most internal stakeholders, be it individuals or teams.

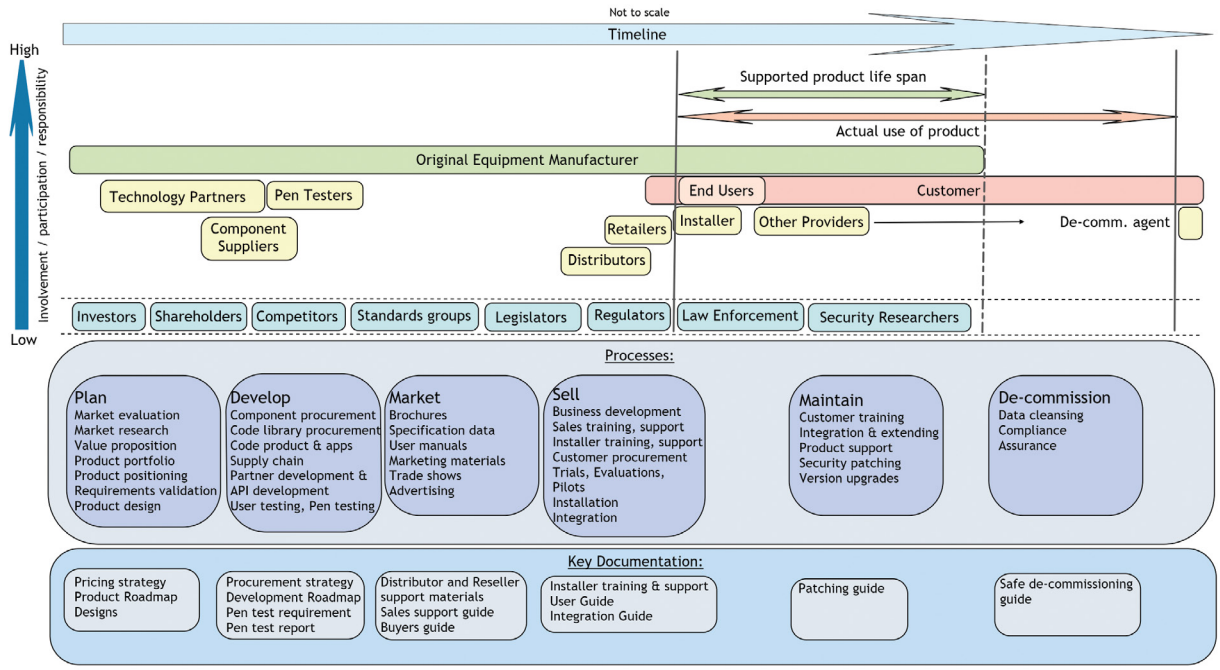
The OEM will have some or all of the following functions to ensure they are in control of the product's business: product manager, designers, developers, marketing, legal, sales & distribution, product support, technical support, etc. A way to explore the needs the OEM's stakeholders have to meet, is to look at the individual stakeholders in the lifespan of the product.

OEM's third party suppliers

Depending on the mix of hardware and software in a product, usually a high percentage of development resources go into software development to create additional value and increase functionality. To facilitate this in today's world there are many third party development libraries for developing new applications. third party libraries often contribute towards 80% or more of the total product code, as such they provide a key role in the security of a product.

In most cases third party suppliers are willing to meet the requirements given to them, including securing components (using secure development techniques for hardware or software), and an independent audit. The supplier will need to know which standards or frameworks are preferred, as well as any mandatory controls to be implemented.

Figure 1.



In some cases, it may seem unrealistic since the OEM may be one customer among hundreds or thousands buying the component / library. However, regardless of the buying power an OEM may have in terms of the overall market, the OEM must participate in user forums, support groups, etc. to push for better security in future versions or move to more secure component suppliers. The hacked product incidents of the last few years has brought this issue to the suppliers' attention and are likely to lead to the market forcing all those who survive to supply more secure components.

The authors believe that over the next few years the understanding, knowledge and experience of security requirements in components by customers will be in favour of the suppliers. Further, the cost of secure components will not add any more to the price.

These beliefs are only likely to become a reality if the OEMs provide the support and guidance including security in their requirements. These must be provided early enough for future versions so they can be included in the design phases. OEMs may also request 'Threat Models' and should provide suppliers with examples of how they can be used to improve security.

Product distribution network

For an OEM to make a fundamental shift from being seen as a surveillance product manufacturer to an enterprise risk and security tool supplier will require a lot of support to the distribution network. Since this network often determines the customer's perception of a product any lack of support materials and training to the distributors will mean a confused message in this market space.

The marketing messages must be clear enough to pass from OEM to distributor, to retailer to customer. Being the closest to customers, retailers must be trained into the business's corporate communications. If they give the impression that they only understand surveillance solutions, they will not be able to convincingly convey the solution vision.

Product training and training into the enterprise security risk needs of customers will be necessary.

Integrators / Installers

One of the lasting impressions a customer has is the knowledge and experience of the installation, and the hand over to the customer by the engineer on site. System integrators and installers play a vital role in any successful project completion; so it is imperative that they are appropriately well trained and supported.

Traditionally integrators and installers of physical security systems are experienced only in surveillance and physical access control i.e. they are experienced in securing physical spaces not technology devices sitting on a secure network.

Given that the operations team and the network staff of most organisations are likely to have far more experience and expertise of securing devices on a network, it is important that installation engineers have a respectable acknowledgement of their limited experience in this field. In most cases it makes good sense for installation engineers to be clear about what they can and cannot secure.

Since an installer may spend the longest time with the customer, it is imperative that they are more than adequately supported and trained as determined by the OEM.

Customer

An enterprise customer is likely to have several stakeholders including: supplier management, procurement, CISO / CSO, risk team, network team, architect, audit, facilities management team, etc. Not only can some of these prolong the procurement process, but they may also delay the installation, and so meeting some of their key security concerns is important.

Each of these stakeholders may be more or less involved depending on the stage of the life cycle of the product. Pre-purchase support and information are important, but no more so than a secure product.

From a security perspective, products must have controls to not only protect them from being tampered with, but to also not compromise other

devices on the network. Additionally, should any vulnerabilities be identified, they must be dealt with so they do not negatively affect the customer for any longer period than necessary.

Customers want an OEM with the capability to provide advice, information and patches in a timely manner soon after a vulnerability is known and before an exploit is available. Along with thiese obvious points, security teams may want assurance that the OEM understands the vulnerability and the response provided.

End users

The end user may or may not be the same entity or group as the customer. It is possible for the customer to be a property company and the end user to be an outsourced guarding company, or for example a CCTV monitoring company. The customer could also be the end user for part of the life span of the product, and the end user could change several times over the period.

Depending on the role of the end user in the overall security of the building or organisation, they may only be involved in an isolated way, or be totally integrated with the whole of security from a converged security management perspective.

However aligned end users are into the rest of the security function, they will still want to be sure that the system can be configured and integrated in the right way without any major issues, and that supporting information is readily available.

Customer's third party suppliers

All organisations use multiple suppliers as part of their enterprise security risk programmes, and several will partner together to provide integrating functionality of systems for more effective and efficient management.

Logical security service providers have long partnered together to provide combined solutions for risk and compliance management. Both physical and logical security providers must work together better if customers are to reap the benefits of a converged approach.

De-commissioning agents are just one of the many third party suppliers, however we included them as a separate group in our diagram, as they are the last party to be involved in finally ending the life of a product even though the responsibility for the product and any data that may have resided on it remains with the data controller.

A customer's other security service providers may influence not just a final solution but how well it integrates with others. Working with service providers whose products interact or overlap can be vital. Many vendors offer lists of products and services their product can be used with.

For example, some physical access control systems can integrate with employee databases and can be used to identify anomalies where an end user is supposedly logged on from abroad but their access card has been used to access the office (or vice versa).

Government & Regulators

The roles of governments and regulators are usually to protect the end user, this can be in stating what must be provided (e.g. as in health and safety), or in what they cannot do (e.g. by making certain acts or activities illegal or unlawful).

The most notable responses have been in guarding staff, or the data protection guidance provided by the ICO for CCTV operators.

Standards groups

Standards groups' experts often include industry members and consumers, and the standards may be a way to improve the industry or products for the end user and their investment in products. Existing standards may influence products from the early stages in design, e.g. the principles around secure by design or data protection by design. New standards will often aim to fill in the gaps in existing standards or new technology areas, for example, although there are several security standards for products, there are already many groups looking at specific products or industry standards for IoT products.

Competitors

The importance of competitors is that they may improve products by driving up quality, security, functionality etc. Most OEMs in the same market space will know each other's products to be able to state what they offer and how they compete.

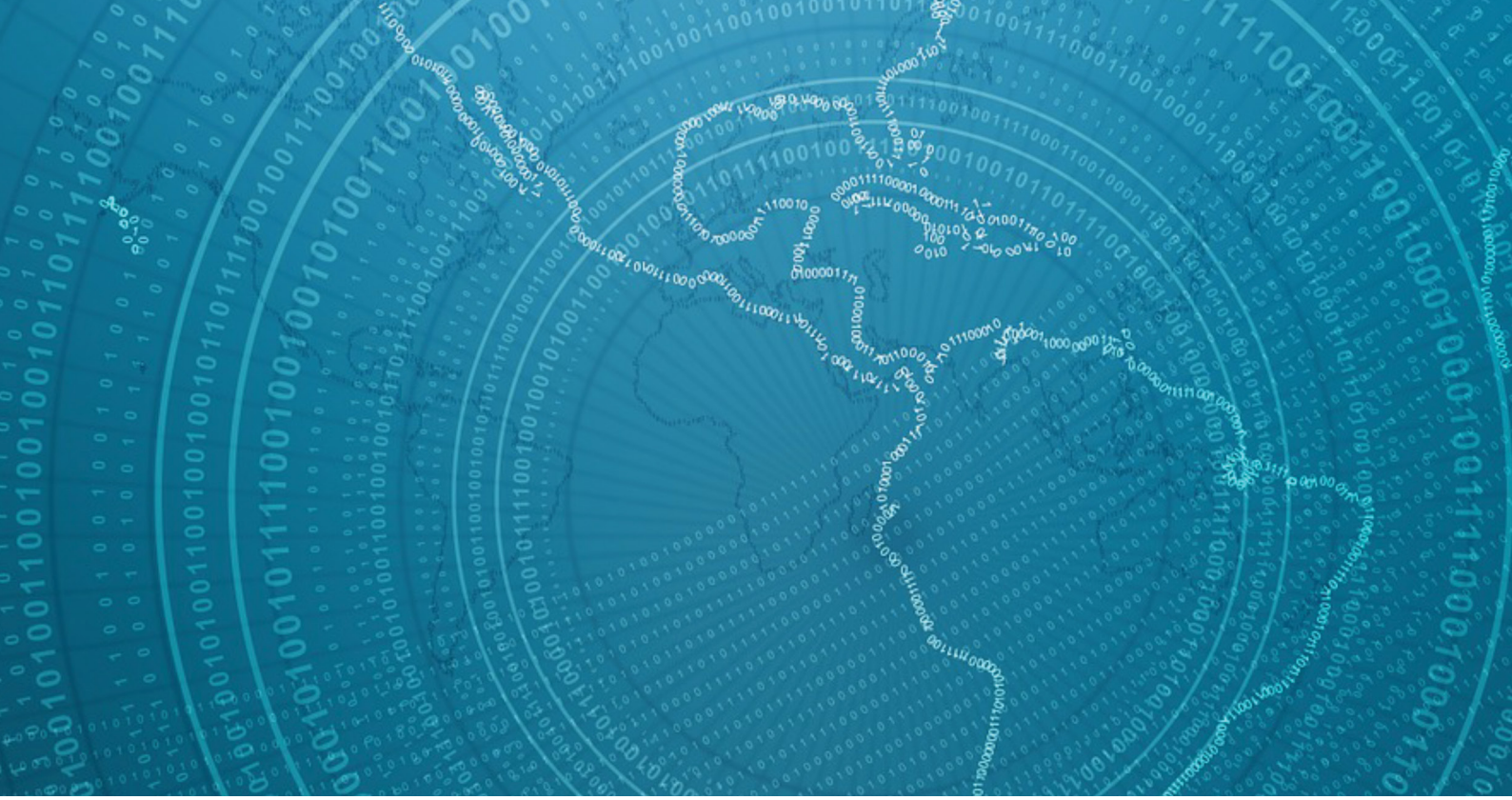
The fact is that if an OEM isn't listening to its customers, then another competitor may do so and develop requirements customers will not only pay for but also will move from an existing supplier.

Others

Law enforcement or security services may want a quick way to collect data directly from the device remotely. Functionality which makes it easier to meet such requests may be beneficial as it can save the end user a lot of time.

Since each stakeholder is likely to experience its own set of changes and challenges to its business, it will have its own specific needs to be able to provide the OEM's vision in meeting the customer's ESRM strategy for CSM.

Royal Oldham training room.



Converged Security Management Requirements

In their work, the Paper's authors have come across many CSOs / CISOs who have believed that their organisation operates CSM, however a few questions often revealed that their impression of CSM was incorrect. This chapter clarifies some of the requirements of CSM.

Convergence, ESRM and CSM

Convergence, which is essentially the bringing together of all security functions to prevent, identify and respond to security risks has been practiced by some leading organisations since the birth of computer security in the 1980s and of course predates that depending on your understanding of technological security. For some a fully converged and integrated security function which oversees all security risks is possible. Tyson, defines it,

"Security convergence is the integration, in a formal, collaborative, and strategic manner, of the cumulative security resources of an organisation in order to deliver enterprise-wide benefits through enhanced risk mitigation, increased operational effectiveness and efficiency, and cost savings" (Tyson, 2007, p. 4).

Others prefer an approach which examines all security risks facing an organisation as part of an enterprise security risk management strategy but does not require a formal single function. ASIS International is focusing on ESRM which it defines as,

"a management process that creates a consistent and holistic approach to managing

threats to any organization through an ongoing process of assessing all security-related risks across the entire enterprise. Under an ESRM framework, security professionals quantify the range of threats, create and implement mitigation plans, identify the appropriate risk owners, manage any incidents that arise, and develop remediation efforts" (ASIS International 2014).

At the heart of both convergence and ESRM is a united multidisciplinary teaming approach which the authors define as Converged Security Management. Deutsche Telekom, for example operates in a single security function. Axel Petri, SVP Security Governance, Deutsche Telekom, writes about his organisation:

"Security has realised that silo solutions won't be successful any longer. Security can only be reached if all stakeholders join forces. This is true for the cooperation between physical and cybersecurity in organisations as well as in national companies that are parts of global groups ... Only if we combine our forces can we be successful in tackling new emerging threats".

In the ANSI ASIS Physical Asset protection standard, this is summed up in a practical way by stating

- In order to understand the shared risk environment, the organization should consider:
- Common lines of communications and reporting for assessing and managing risk in a cross-disciplinary and cross-functional fashion
- Establishing cross-disciplinary and cross-functional teams to achieve a coordinated pre-emptive and response structure.

(ASIS International, 2012, p xiv).

The National Institute of Standards and Technology (NIST 2016) has also recognised that an integrated risk management approach is required in the design and operation of IoT which emphasises trustworthiness and reliability. It argues that each area of a company needs to discuss their systems with one another in the manufacture and implementation of a device.

"Security convergence is the integration, in a formal, collaborative, and strategic manner, of the cumulative security resources of an organisation in order to deliver enterprise-wide benefits through enhanced risk mitigation, increased operational effectiveness and efficiency, and cost savings."

Hence the Heads of Privacy, Resilience, Security, Safety and Reliability need to discuss cyber security risks. This applies both to vendors and end-users. It cites cyber security as the key area of concern for all systems and only a collaborative response will identify and manage the impact of these risks (p 82f).

To date the focus has been on cyber security technology being used to identify these attacks but senior security professionals now agree that a united cyber physical security response will be more effective than a reliance on the cyber security function alone.

10. Tyson, D. (2007), Security Convergence: Managing Enterprise Security Risk, Burlington, MA: Elsevier Buttterworth-Heinemann
11. ASIS International (2014): Enterprise Security Risk Management. A Holistic Approach to Security, ASIS International, CSO Roundtable.https://cso.asisonline.org/esrm/Pages/default.aspx. accessed 29/05/2017
12. ASIS International (2015) ASIS 14TH EUROPEAN SECURITY CONFERENCE & EXHIBITION: AN INTERVIEW WITH AXEL PETRI. https://sm.asisonline.org/Pages/Q.-and-A.-Axel-Petri.aspx
13. ASIS International (2012) ANSI/ASIS PAP.1-2012, Security Management Standard: Physical Asset Protection.
14. NIST (2016) Cyber Physical Systems Public Working Group: Cyber Physical Systems Framework, May 2016.https://pages.nist.gov/cpspwg/ accessed 29/05/2017

The Perpetuity Research Initiative surveyed 289 cyber physical security leaders from across the globe and found that '56% favoured a single team against 38% separate and 6% unsure as their preferred way to organise security'. (Perpetuity Research Initiative, 2016, p 44). This provides the vendor with a great opportunity, to enable and enhance the enterprise security team with converged technology which identifies the blended attacks and strengthens an organisation.

Leveraging converged security technologies

How can technology be leveraged to be more effectively used by physical and logical security and empower a converged strategy? Some large companies have successfully deployed Physical Security Information Management (PSIM) systems which integrate the data from all physical systems and co-ordinate a response to an incident with far better results than when those systems operate separately. Hence a fire can be managed more effectively when all the available data and controls are integrated. But very few companies currently use the logical security equivalent to identify and respond to cyber attacks on their physical systems.

In fact, Security Incident Event management (SIEM) systems can be configured to do this. It means if a breach occurs on a system that once identified it can be monitored and managed such that the system can be restored much more quickly.

Key action points for the management of converged security technologies.

- It is important that organisations appreciate that there are converged threats on their cyber physical systems and they have a technically converged response
- Plan a fully integrated SIEM/PSIM which links all security systems and alerts multi-disciplinary security teams to cyber physical attacks - this will help in breaking the silos of security risk management and enable a near real time response
- Design and build 'joint' cyber physical security operations centres following the example of some forward thinking companies.

For those who still wonder why we should do this, Eugene Kaspersky, a global expert on malware, said at the World Economic Forum in January 2016, "Cyber is physical. It's everywhere around us. Even the cameras which are recording us, they are cyber" (WEF, 2016).

Benefits of multi-disciplinary teams using converged technologies

These converged technologies which have the potential to make such a difference need multi-disciplinary cyber physical security teams to understand and respond to the alerts they produce. Converged teams operating in the way the ASIS PAP Standard recommends can monitor converged technology in areas such as physical and logical access. This type of solution has existed for over a decade but even where it is used to manage access and provide clear audit trails often the data is not utilised. This is where automotive intelligent solutions can assist by alerting security teams to anomalies and disable passes to prevent unauthorised access until they are assessed. It might be that the person has left the company and someone else is using their access but unless the pass is programmed to decommission it remains active. The significance is in the use of a more converged technology which identifies access to all systems managed by a cross functional team.

15. Gill, M, Howell, C (2016) Tackling Cyber crime and the role of Private Security (A Security Research Initiative) Perpetuity Research and Consultancy International (PRCI) Ltd https://perpetuityresearch.com/wp-content/uploads/2016/09/SRI-Report-2016.pdf accessed 29/05/2017.
16. Kaspersky, E (2016) - Press Conference: Confronting Cybercrime - A Public-Private Partnership: https://www.youtube.com/watch?v=f0zMJ_C8YRU

Benefits of teaming

- A cross functional security team can also benefit from AI which helps predict future attacks based on past incidents and available data on the current threat landscape
- All this data needs to be brought together so that the physical and logical systems are integrated because the boundaries between physical and logical no longer exist
- Blended risks are fully understood and mitigated so that businesses will see the value of protecting the cameras, BMS and other physical systems on the network from a cyber attack.

If a business can give evidence to the UK Information commissioner's office that there is a strong CCTV information and cyber security policy in place then the risk of heavy fines for breaches caused by CCTV vulnerabilities will be reduced. It is all very well to have the most advanced technical controls but unless these are managed appropriately then the company doesn't benefit. The World Economic Forum emphasised

"It is vital to integrate physical and cyber management, strengthen resilience leadership and organizational and business processes, and leverage supporting technologies". (WEF 2016, p 18).

It is these teams which will determine the cyber physical security risks posed by IoT devices through the use of converged solutions and a unified response.

They will have sufficient expertise and experience to assess the alerts raised by the converged solutions and in the future work alongside AI to achieve a consistent and effective response to cyber physical threats. One of the leading cyber security gurus of the 21st century, Bruce Schneier stated at Information Security Europe in 2016, "Sony was hacked because there was no teaming in the organisation in either the defence or the response". This really is the point. You can have the best Chief of Security but unless they establish multi-disciplinary teams and converged technological solutions to defend and respond to cyber physical attacks then it doesn't matter as sooner or later your organisation will be breached.

17. World Economic Forum (2016): The Global Risks Report 2016. http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf accessed 29/05/2017.
18. Schneier, B (2015): InfoSecurity Europe: Keynote Stage - How Do You Know You've Been Breached? http://www.infosecurityeurope.com/en/media/video-channel/2015-keynote-videos/ Accessed 29/05/2017.

Exterior outdoor cams.

Vendor Support

Any business large or small only purchases security products and services in the context of their response to managing risks more efficiently and sometimes also effectively.

As was illustrated in Chapter 1 both business and criminal worlds are moving at a very fast pace and the risks businesses are exposed to are changing too.

One of the responses by security teams is to deal with the changes and manage security risks to bring together the various security and resilience functions into a single unified team.

So any conversation with security teams must be about solving their problems, not about introducing more challenges for them. The 'old school' sold to physical security and sometimes created problems for network and security teams.

Traditionally physical and logical security solutions have been sold into siloed teams, however with technology convergence in most organisations any technology which is expected to sit on the network must be agreed with at least a couple of network / security managers.

The support from a vendor to facilitate converged security management in an enterprise is related mainly to answering questions the logical security team have and cannot be answered by the physical security team. The more these questions are answered either in direct literature from the vendor or on behalf of the vendor, the better it is for the logical security team, as they are able to ask questions directly rather than go via the physical security team.

Whilst accepting that no single approach or list of concerns will be the same for every customer in

every industry to help them meet their risk and compliance concerns, there are two related areas of interest to logical security teams. It is important to remember that the contents of these lists are not intended to provide specific guidance on the security of IoT devices, but offer high level guidance on actions or changes that will be recognised and appreciated by logical security teams to convey that a vendor is taking the security of its IoT devices at least as seriously as logical security vendors are considered to be doing.

Product Information & support

Overall the product information and support must be aligned with the customer's enterprise risk needs for the product lifespan from the pre-sales or marketing information from pre-purchase to the de-commissioning information.

- The risk management message must be consistent throughout the supply chain conveying the solution space as enterprise security risk management tools rather than surveillance tools.
- Provide information on how to specify this range of tools/products (or requirement documents) so that security is either already built into the product, or at least there is an effective road map to build security in over the life span of the product.
- Training is provided to appropriate marketing and pre-sales staff so they are able to answer questions on what levels of security are built into each product and have a clear understanding of additional controls that need to be applied to lock the device(s) down further (for additional security).
- Information on suggested architecture for secure installation and network operations is also important as network and security teams are able to understand how the products will fit into the existing architecture and networks, and what impact if any they may need to be concerned about.
- Installation partners / staff must be trained (beyond a novice level) in network security practices so that they are able to have an intelligent conversation on the state of network controls implemented or required. Transparency of installer skills maybe necessary. Further, on any additional actions which may need to be applied for enhanced security. Where vendors are unable to provide installation partners with the appropriate level of network security, the installer should either be on the road map to rectify this or the customer should be informed at the outset that the installer is only experienced in basic system set up excluding any network connection.
- All relevant stakeholders who interact with the customer must understand that it is more professional to admit that one doesn't know and that they will find out than to try to impress with inadequate information.
- Regular communication relating to the implications of news items and discussions on how customers can ensure that they are not vulnerable to the "bad stuff" that goes on in the world helps provide reassurance without the customer having to look for such information.

From a compliance perspective, it is reassuring for enterprises to know that any vendor is facing and dealing with some of the issues in a similar way, as they would in house. Any good practices a vendor is able to share will go a long way to demonstrate that a vendor actually understands the compliance issues rather than to just say that they do.

Product security

When it comes to product security, logical security teams are likely to be more interested or concerned about some of the following.

- Secure development processes / standards must not only be used, but there should be a (policy) to ensure that key third party suppliers of components and code also have their own equivalent policies. These processes

/ standards provide a level of assurance that some of the obvious easy to find bugs are likely to have been picked up without the need for unnecessary patching later., There also needs to be a clear statement to show a willingness to replace any component suppliers who do not follow the relevant processes / standards, Where a vendor's secure development processes are better than a customer's own processes, they will generate greater respect than if it is the other way around.

- Where a device interacts with several layers of the OSI model, it may be necessary to consider the security of each layer and any additional controls which may be required, rather than to assume that all controls should be at one level – the network level. This does imply that each new layer introduced may require its own threat model, for example where an embedded web server is used, a complete threat model on that web server may be appropriate.
- Where penetration testing services are used, providing testers with all the code and threat models may help question the assumptions made and provide more useful responses, as well as another group of testers testing blind.
- Where additional controls like encryption are included in the product, not only should the most recent standards be used, but also the relevant guidance for implementing these must be used. There may also be a need to provide some assurance that implementation has been applied correctly. Proprietary encryption should never be used.
- A responsible vulnerability disclosure policy and practices are important, and (disclosures) should follow standard industry guidance.
- A responsible patching policy is also important, as exampled by Microsoft recently, which may mean that patching a product that is no long supported is for the good of everyone. Timely patches with the right communication and functionality to automate them are vital. Patching several tens, or hundreds of devices individually is no easy task, the functionality to manage all of these and know which ones are patched, what patches are on them and when they were last patched is also important.
- When it comes to patching, it isn't just how vendors deal with any code developed in-house but also how the vendor deals with patches to code in important third party libraries, and how it ensures that such patches do not leave the customer vulnerable.

Author Biographies

James Willison
BA MA MSyI

James is Founder of Unified Security Ltd and Vice Chair of the ASIS European Convergence/ESRM committee. James was awarded the Imbert Prize for an 'outstanding contribution to the Security Industry in 2011' for his work on convergence with ASIS Europe and the Information Security Awareness Forum. He has worked with BP, Loughborough University, Mitie TSM, the EU and AXIS Communications on convergence. He is an ISACA Academic Advocate and a member of the draft ASIS/ISACA/ISC(2) Security Awareness Standard' Working Group. Unified Security Ltd provide consultancy which is designed to ensure organisations align their support functions and in particular the areas of Physical and Information Security. This includes security policy, common reporting processes, converged security risk assessment, training courses and White Papers.

Sarb Sembhi CISM

Sarb is the CTO & CISO at Virtually Informed, and has previously been a CTO & CISO for the Noord Group. He has previously worked as a consultant covering most issues in risk and security. Sarb's contributions to the industry include the London Chamber of Commerce and Industry Defence and Security Committee and its Cybersecurity working group. Other contributions include: Past President of the ISACA London Chapter, Chair of ISACA International GRA Region 3 Sub-Committee, Chair of ISACA International GRA Committee, ISSA UK Advisory Group member, InfoSecurity Magazine Editorial Group member. Sarb has also served on several Security Standards Groups, and continues to write and speak at risk and security events around the world.

Sarb was shortlisted in the IFSEC Global Most Influential people in Security & Fire 2017: www.ifsecglobal.com/top-50-influencers-security-fire-2017-cybersecurity

Unified Security Limited

Randall Villa, Dartford Road, South Darenth
Dartford Kent DA4 9HY.

Tel: +44 (0)1322 862901 / +44(0) 7841 716342
Email: jameswillison@unifiedsecurity.net