Staying cyber safe in industry

euautomation

In 2014, the total number of cyber security incidents detected rose to 42.8 million according to pwc's global state of information security survey 2015. For those of you that have not done the maths, that is 117,339 attacks per day, every day. And these are just the strikes that were detected and reported.

To comprehend the sheer extent of current threats, antivirus business Kaspersky has created an interactive map. It depicts the number and type of cyber threats in real time. If you are reading this white paper online, I am sure you will agree that it is almost hypnotic. If you are reading offline, I recommend you visit http:/cybermap.kaspersky.com.

But the map is also incredibly worrying. The total number of security attacks detected increased by 48 per cent from 2013 to 2014 and there is little evidence to suggest this percentage will decrease in 2015. Despite these figures, it appears that information security programs have actually weakened, due largely to naivety and inadequate investment.

In the industrial sector alone, companies reported a 17 per cent increase in detected security incidents in 2014. The resulting financial costs increased by 34%, while research from Barclays suggests that nearly 50% of businesses that suffer a cyber security attack cease trading.

This special report analyses the increasing global cyber threat and outlines the value of implementing a business focussed security strategy to ensure the wellbeing of both employees and industrial automated systems.

Who done it?

The year 2014 featured some of the biggest hacking and cyber security breaches of the decade. It seems nobody was safe, not even the biggest corporate players. eBay, Sony Pictures Entertainment, Apple and Sony Playstation, were all victims of cyber attacks in one form or another.

Interestingly, there is one thing most security threats have in common and that is the source. The results of PWC's survey illustrate that 34.55 per cent of companies asked, reported that the attacks on them last year were estimated to originate from current employees of the company and 30.42 per cent from former employees. These were the two biggest culprits.

Statistically, you are far more likely to come under cyber attack because of someone plugging in a corrupted USB stick to your network, than you are to be specifically targeted by a hacker trying to exploit a weakness in an automated system. However, that's not to say that you shouldn't prepare for both eventualities.

Hackers still ranked highly in the survey - third with 23.89 per cent of companies surveyed pinning their security attacks on them. However, there is another, less prevalent threat that companies should be aware of too.

Every business encounters third parties on a daily basis - such as consultants, contractors, suppliers and providers. It is imperative that the information shared with these parties, on and off site, is restricted to an appropriate level. 18.16 per cent of businesses surveyed responded that they believed their current third party providers were responsible, actively or passively, for their cyber attacks.

For example, the US retail giant Target had a considerable breach in 2013 when the personal identifiable information (PII) and credit card details of customers were stolen. The multi-staged hack began with Target's heating, ventilating and air conditioning supplier, who, it would seem, had access to Target's network. Credentials were stolen from the US vendor using common malware implemented through an e-mail phishing campaign. This was the hackers' way in.

The moral of the story is that to develop secure systems, companies must implement technical, conceptual and organisational measures to prevent different types of security threats.

Where to start

In a manufacturing context, typical security incidents include infection by malware, unauthorised use, manipulation of data, espionage and denial of service - the latter being an attempt to make a machine or network resource unavailable for its intended users.

Defence against these kinds of threats takes more than simply investing in new software or hiring a Chief Information Security Officer (CISO), although these measures are a good start. Changes need to be implemented from the ground up. Before we get ahead of ourselves there are certain steps that should be taken prior to anything else.

To evaluate properly the likely threats, system owners must first assess the weak points of that system - including the human element. In an automated environment, this may reveal a scenario in which a property of the whole is considered beneficial from an automation perspective, but detrimental from security one.

For example, a remote device that is free to gain access to a programmable logic controller (PLC) without authentication saves time in an automated process. However, from a security perspective this is a definite weak point. It is necessary to identify these weaknesses in order to access risks and take appropriate action.

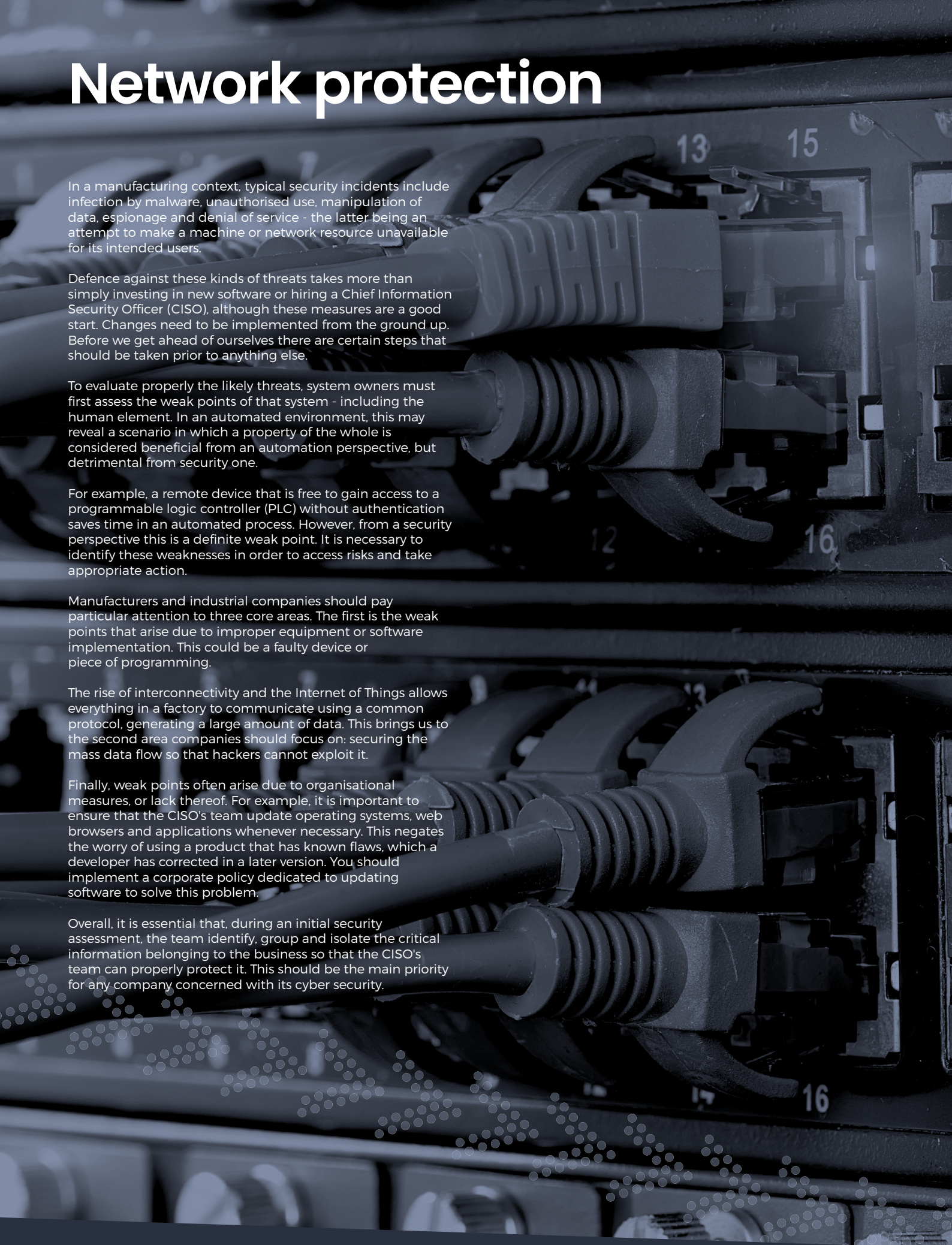
Manufacturers and industrial companies should pay particular attention to three core areas. The first is the weak points that arise due to improper equipment or software implementation. This could be a faulty device or piece of programming.

The rise of interconnectivity and the Internet of Things allows everything in a factory to communicate using a common protocol, generating a large amount of data. This brings us to the second area companies should focus on: securing the mass data flow so that hackers cannot exploit it.

Finally, weak points often arise due to organisational measures, or lack thereof. For example, it is important to ensure that the CISO's team update operating systems, web browsers and applications whenever necessary. This negates the worry of using a product that has known flaws, which a developer has corrected in a later version. You should implement a corporate policy dedicated to updating software to solve this problem.

Overall, it is essential that, during an initial security assessment, the team identify, group and isolate the critical information belonging to the business so that the CISO's team can properly protect it. This should be the main priority for any company concerned with its cyber security.

Network protection



In a manufacturing context, typical security incidents include infection by malware, unauthorised use, manipulation of data, espionage and denial of service - the latter being an attempt to make a machine or network resource unavailable for its intended users.

Defence against these kinds of threats takes more than simply investing in new software or hiring a Chief Information Security Officer (CISO), although these measures are a good start. Changes need to be implemented from the ground up. Before we get ahead of ourselves there are certain steps that should be taken prior to anything else.

To evaluate properly the likely threats, system owners must first assess the weak points of that system - including the human element. In an automated environment, this may reveal a scenario in which a property of the whole is considered beneficial from an automation perspective, but detrimental from security one.

For example, a remote device that is free to gain access to a programmable logic controller (PLC) without authentication saves time in an automated process. However, from a security perspective this is a definite weak point. It is necessary to identify these weaknesses in order to access risks and take appropriate action.

Manufacturers and industrial companies should pay particular attention to three core areas. The first is the weak points that arise due to improper equipment or software implementation. This could be a faulty device or piece of programming.

The rise of interconnectivity and the Internet of Things allows everything in a factory to communicate using a common protocol, generating a large amount of data. This brings us to the second area companies should focus on: securing the mass data flow so that hackers cannot exploit it.

Finally, weak points often arise due to organisational measures, or lack thereof. For example, it is important to ensure that the CISO's team update operating systems, web browsers and applications whenever necessary. This negates the worry of using a product that has known flaws, which a developer has corrected in a later version. You should implement a corporate policy dedicated to updating software to solve this problem.

Overall, it is essential that, during an initial security assessment, the team identify, group and isolate the critical information belonging to the business so that the CISO's team can properly protect it. This should be the main priority for any company concerned with its cyber security.

Security via education

Part of the current problem is that the topic of cyber security isn't being elevated to a board level discussion in most companies despite the damaging consequences of security breaches including loss of production, reduced product quality and safety threats to both humans and machines.

Most governments have created or are in the process of creating, cyber security regulations that impose conditions on the safeguarding and use of PII. Companies that fail to sufficiently protect sensitive information risk financial penalties. Despite this, some companies remain ignorant.

Regulations are particularly prevalent across Europe and should serve as an example of what countries that do not yet have legislation should expect in the near future. The US also has mandatory conformance policies when it comes to companies protecting PII.

At the beginning of 2104, the US implemented a framework for improving cyber security infrastructure: a set of industry standards and best practices aimed at helping organisations manage cyber security risks. However, these measures have been heavily criticised for not going far enough, especially in light of the recent high profile Sony Pictures Entertainment hacking scandal allegedly involving North Korea.

To help educate businesses in the ways of information security, the UK Government has allocated £860 million until 2016 to establish a National Cyber Security Programme. Part of this agenda is to ensure the UK is one of the most secure places to do business online. This comes after it was revealed that 81 per cent of large corporations and 60 per cent of small businesses in the UK reported a cyber breach in 2014.

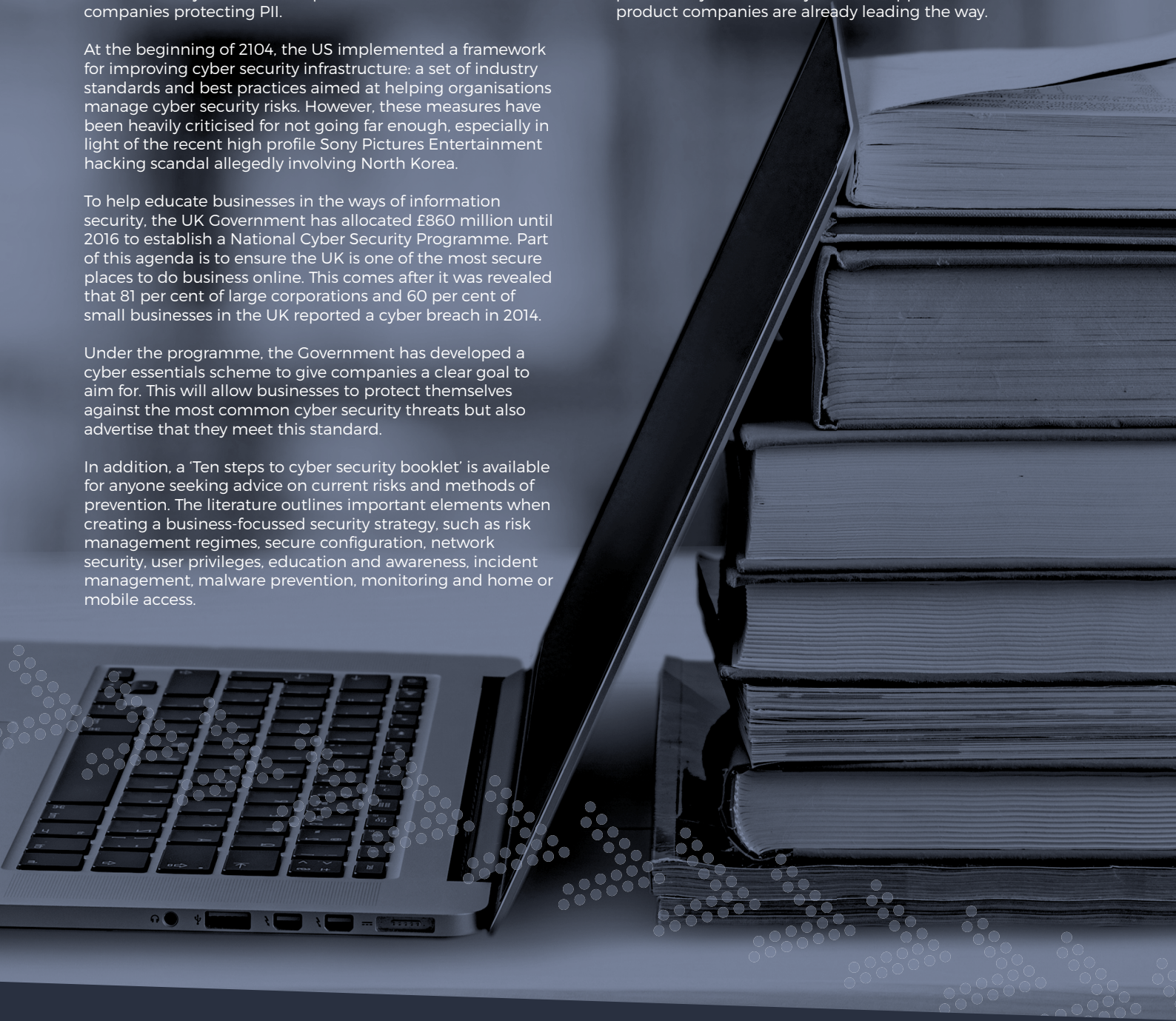
Under the programme, the Government has developed a cyber essentials scheme to give companies a clear goal to aim for. This will allow businesses to protect themselves against the most common cyber security threats but also advertise that they meet this standard.

In addition, a 'Ten steps to cyber security booklet' is available for anyone seeking advice on current risks and methods of prevention. The literature outlines important elements when creating a business-focussed security strategy, such as risk management regimes, secure configuration, network security, user privileges, education and awareness, incident management, malware prevention, monitoring and home or mobile access.

Businesses that want to find out more about how to increase their security levels can also access a useful guideline document from the industry standards agency PROFIUBUS & PROFINET International (PI).

The Security Guideline for PROFINET was originally developed in 2006 and later revised at the end of 2013. It specifies ideas and concepts regarding how and which security measures should be implemented. It also contains a list of commonly used security acronyms and offers a series of proven best practices, such as the cell protection concept mentioned earlier.

The information is out there for companies seeking advice regarding cyber security. However, from the statistics provided by PWC's survey, it would appear that industrial product companies are already leading the way.



Industry

On the whole, cyber threats are increasing and yet information security budgets seemed to decrease in 2014. The industrial products market is the exception because it has created budgets to protect itself.

According to the PWC security survey, this sector, more than all other surveyed - power and utilities, healthcare, retail and consumer, technology and financial services - appears to understand rising security risks. Moreover, it's investing accordingly.

Information security budgets for industrial products companies have soared more than 150 per cent in the past two years. In 2014, information security spending represented 6.9 per cent of PWC survey respondents' total IT budget, the highest of any sector surveyed. However, in 2014, security incidents in the sector also increased six fold. So perhaps even a 150% increase is not enough.

The result of this investment has been notable improvements in security processes and technologies, as well as training initiatives. However, there is still generous room for improvement.

Stay safe

Megatrends such as Industry 4.0, the Internet of Things and big data have driven industrial automation to a completely new level, creating more efficient and sophisticated production lines. Industry is integrating its manufacturing lines with IT layers and the traditional industrial automation pyramid is collapsing due to the need for faster, cheaper and more effective production. However, there is a price for these gains: with greater openness, interconnectivity and dependency comes greater vulnerability.

There is a definite need for more training when it comes to cyber security, both at the top and bottom of the manufacturing ladder. Too often businesses slip into common pitfalls - believing they are either untouchable or not a target.

If the majority of cyber attacks in 2014 were committed by current employees of the affected company, how many of these do you think were undertaken knowingly? Or were they the result of an individual not fully understanding that his or her actions could lead to security breaches?

Understanding that you don't have to be a desirable target for hackers and that cyber threats can be the result of non-malicious, poor judgement from one employee is key to understanding the risks.

Even if management wholeheartedly implements a dedicated cyber security downwards, all it takes is one malware-infected device plugged into the network to cause disruption. We cannot prevent accidents, but it is possible to manage them by instilling knowledge in employees and putting in place reliable monitoring devices and procedures for when an attack occurs.

Security training shouldn't be limited to a one off seminar for the staff and an initial systems upgrade. Patch maintenance and updates need to be carried out as and when vulnerabilities are revealed or new software is released. Senior management need to implement vigorous maintenance and monitoring policies. Security is a constant and evolving concern, not something that can be solved with one quick fix.

Risk assessments need to be undertaken for suppliers, providers and contractors and restrictions on information should be put in place. Again, this can't simply be an initial appraisal. Unified procedures should be written up and followed when dealing with any third party that requires a certain level of information from a business.

With financial investment and appropriate attention paid to cyber security infrastructure and procedures, a business will be ready should a malicious external attack take place. Otherwise, a company does not just face loss of production and financial penalties; there is also loss of reputation and potential danger to both machines and humans to consider.