SIEMENS
Ingenuity for life

Frost & Sullivan

Protecting Business Continuity Against Cyber Threats

A Siemens Building Technologies Whitepaper

siemens.com/bt/security

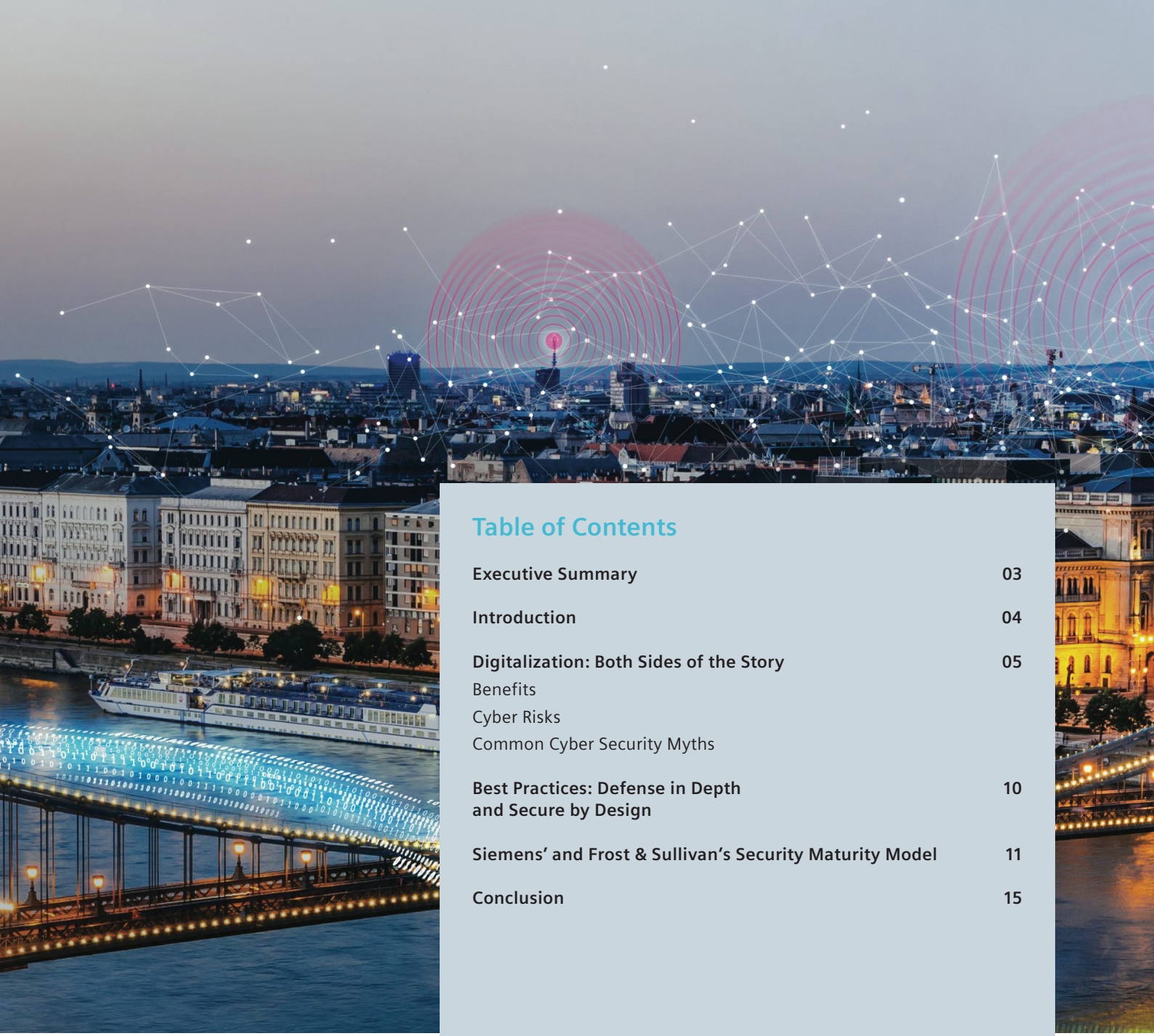
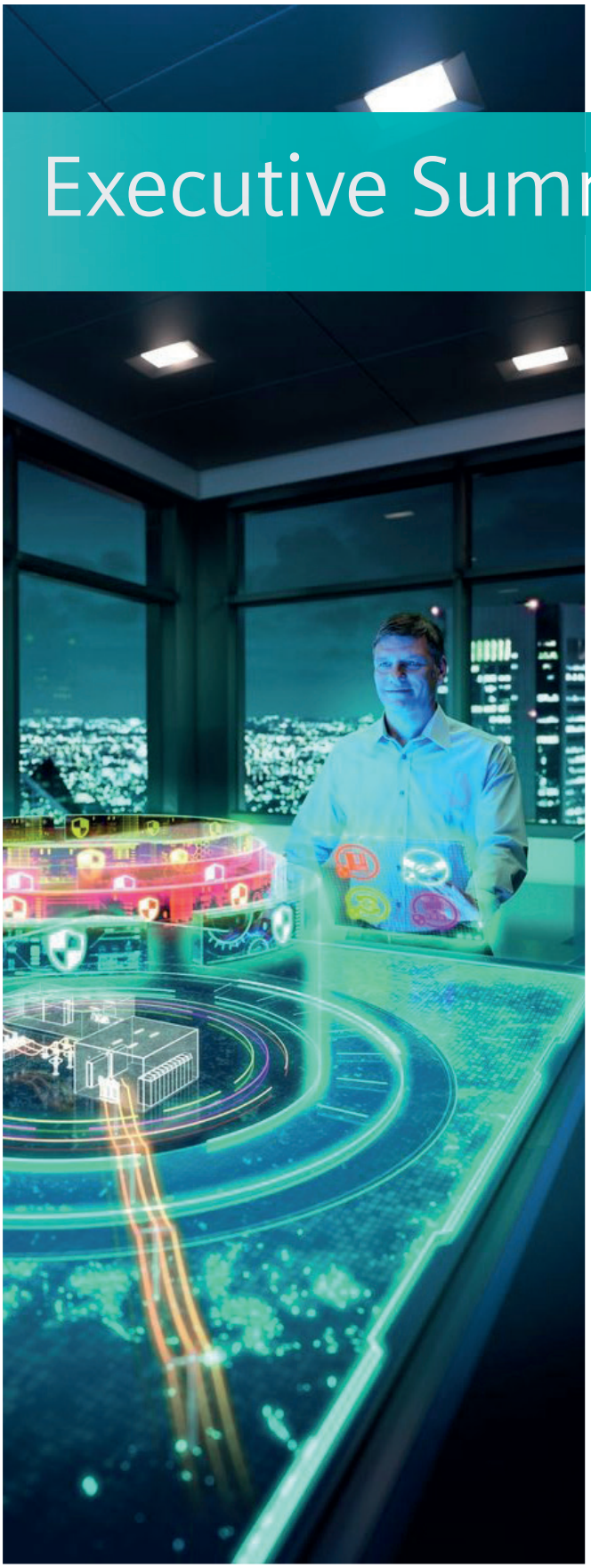


Table of Contents

Executive Summary



Gone are the days when cyber attacks only threatened a company's information technology systems. Today, operational technology systems are also at risk. Thanks to the interconnectedness of operational and information technology as well as the increasing number of intelligent devices, there are many more points of entry into a company's systems. And now when hackers find the weakest point to target, they can gain access to the entire building system. In the worst case scenario, your operations can be brought to a halt. The immediate impact can be significant – your financial losses can average USD300,000 per hour if your organization has more than 1,000 employees according to a recent survey by ITIC.[1] It is even more in the financial services industry, where losses can be £100,000 a minute if a trading floor is unexpectedly closed, according to Frost & Sullivan.[2] But that can be just the beginning. Your reputation and brand can be damaged as customers lose confidence. Insurance premiums can be increased. Fines can be levied by regulatory authorities if your company did not take adequate preventive action. Furthermore, any business can be vulnerable to an attack. It is a myth that smaller organizations are not targeted. For them, a cyber breach could mean the loss of intellectual property that damages fundamentals of the business going forward.

Continued vigilance is vital. It is not enough to install a solution and then stop monitoring the systems and connected devices. Cyber resiliency requires a systemic commitment that starts at the top with the board of directors and C-level executives and then includes the entire organization. This paper explores cybersecurity and the steps to take to ward off potential threats.

1 http://itic-corp.com/blog/2017/05/hourly-downtime-tops-300k-for-81-of-firms-33-of-enterprisessay-downtime-costs-1m/
2 Frost & Sullivan – Research

Introduction

While there is a lot of hype around the topic, cyber threats are real and the threat landscape is constantly evolving. Although it is never possible to be 100% secure, the right preventive action can minimize risks. And you can be certain you won't be alone in looking for the right cybersecurity solutions for your organization. Frost & Sullivan forecasts that worldwide spending on security for critical national infrastructure (CNI) alone will reach USD68.98 billion in 2018, up 8.13% from previous year spending. Security spending for areas not defined as CNI is estimated to add an additional USD21 to USD24 billion to security spending in 2018.[3] Spending is increasing in large part because of the risk of security breaches. But it is also being driven by the ongoing digitalization of business.

In search of greater business productivity and operational efficiency, enterprises like yours are deploying ever-increasing numbers of intelligent products and solutions. More and more critical building systems are now networked to allow remote management and monitoring. Securing all of these assets is important because they open up new avenues of cyber risk across both the operational technology (OT) network and the information technology (IT) network. The OT network is used to monitor and control how physical devices perform.[4] The IT network is used to manage and maintain email, laptops, servers, and business software that all employees use. While these two networks were kept separate in the past, they now communicate with each other, which can lead to cross-contamination. The interconnectedness also gives cyber adversaries more places to look for weak points that enable access.

Increased interoperability between IT and OT means the weakest point can enable access to the entire building system.

For example, when an IT network is breached via malware or social engineering[5] subterfuge, it gives hackers, rogue employees or cyber criminals access to the building and its networked systems. This means that a breach started on an employee laptop could not only compromise data in one department, it could eventually lead to unauthorized control of the comfort system, the internal lighting system, the fire safety system, the identity and access control system and so on. Unfortunately, the majority of organizations focus exclusively on protecting IT systems and fail to recognize the risk associated with networked OT systems. The losses can be significant.

USD300,000 per hour – Average loss cited by 81% of respondents in a recent ITIC survey.

£100,000 per minute – Loss to a financial services company if a trading floor unexpectedly closes.

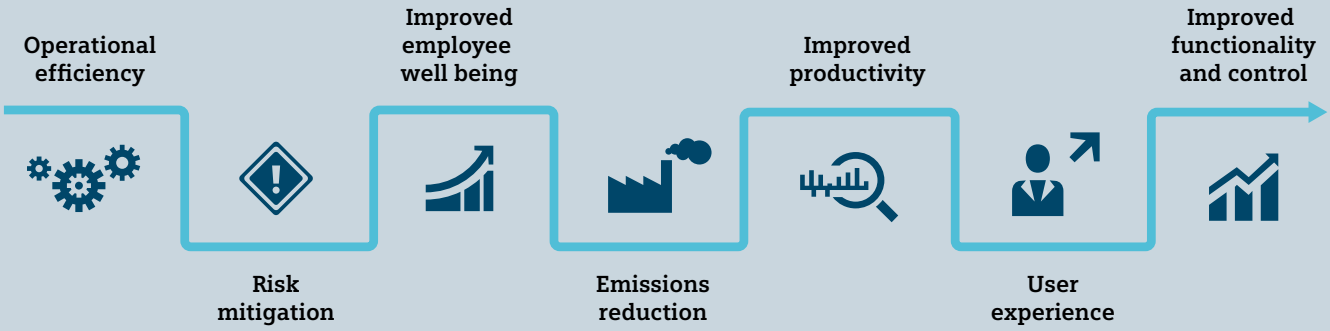
In light of these risks, it is important that facility management teams have the tools and adequate budgets to guard against potential cyber threats that can disrupt any or all of the operations in a building. This is true for companies of any size, not just large ones. From hotels that use electronic door keys, to fully networked factories, to campuses for corporate headquarters, hospitals and universities, all are potential targets. While the risks are real, so are the benefits of digital technology. Smart corporations don't let cyber risks keep them from the advantages to be had from digitalization.

3 https://www.dhs.gov/critical-infrastructure-sectors
4 http://whatis.techtarget.com/definition/operational-technology
5 https://www.csoonline.com/article/2124681/social-engineering/what-is-social-engineering.html

Digitalization – Both Sides of the Story

Digital technology has been transforming the way we live and work and will continue to do so. There will be 60.7 billion connected devices worldwide by 2024, according to Frost & Sullivan[6], and the amounts of data generated will further revolutionize industries across the board. The convergence of OT and IT and the emergence of reliable cloud based solutions are enabling the development of software as a service (SaaS) offerings. In addition, buildings are becoming smarter all the time and we are seeing the growth of smart cities that include a dynamic "internet of buildings."

Exhibit 1 – Key Benefits of a Digital Building



Benefits

The benefits of building digitalization are plentiful, including the following key advantages:

1 Operational efficiency

Facility management teams can now make operational decisions based on building data. For example, occupancy data generated by sensor networks supports real-time operational decisions about heating, ventilation, air conditioning, lighting and shading.

2 Risk mitigation

Interconnectivity of disparate building systems – from fire and security to elevators and doors – enables a concerted response during events, improving safety and security. The integration of security systems with intelligent access control also allows for effective zoning of buildings to ensure only the right people have access to the right areas.

3 Improved employee well-being

There is increasing awareness that creating an optimal working environment for employees can lead to improvements in happiness, well-being and, ultimately, productivity.[7]

4 Enhanced user experience

People are now accustomed to immediate communication via their smart devices – from phones to tablets to wearables such as smart watches and activity trackers – and want the same when they are at work. In an office, for example, employees can be alerted to emergencies, offers in the cafeteria, or scheduled presentations and events that could be of interest.

5 Emissions reduction

With buildings accounting for approximately 40% of global carbon emissions, improving energy management and efficiency is a core policy objective for many countries and companies. Advanced building energy management systems (BEMS) can significantly reduce energy consumption, while providing detailed data and insights into overall performance.

6 Improved business productivity

Companies increasingly expect building technology to improve not just the efficiency and performance of their buildings and assets, but also the productivity of their businesses. The convergence of automation technology, tools for workplace design and optimization, and facility management software is leading to actionable data that helps improve business performance metrics.

7 Improved functionality and control

Digitalization brings opportunities for higher levels of functionality and control. This covers everything from the personalization of hotel rooms to centrally managed identity and access. This creates more data, which requires an intelligent management layer for the building automation systems that are increasingly moving into the cloud.

6 Frost & Sullivan – Total Internet of Things (IoT) Device Forecast, 2014 – 2024
7 "Operations & Maintenance Best Practices: A Guide to Achieving Operational Efficiency," Federal Energy Management Program, U.S. Department of Energy, August 2010 | 8 http://www.aon.com/2017-global-risk-management-survey/

Cyber Risks

The same advances in connectivity and digitalization that bring clear benefits also increase a company's exposure to cyber risks, which have become top of mind in recent years. In 2013, cyber crime was ranked number 18 in Aon's biannual Global Risk Management Survey but came in at number 5 overall in 2017[8]. Different regions saw it differently in 2017: it was ranked the number 1 business risk in North America, but was number 6 in Europe, number 7 in APAC, and number 8 in the Middle East and Africa. When asked about their cyber risk assessments, survey respondents said that they are mainly conducted by the information technology department. Only 13% of respondents said the operations department was actively involved in cyber risk assessments despite the pivotal role it plays in both digitalization and combatting cyber threats.

The operations department was actively involved in only 13% of total cyber risk assessments despite the pivotal role it plays in both digitalization and combatting cyber threats.

Exhibit 2 – Potential Impacts of a Cyber Attack

Building Interruption Resulting From Operational Issues

For a critical function this can result in significant financial losses in many industries

High Insurance Premiums Issues

Insurers are increasingly focused on whether companies have adequate cyber protection and punish breaches

Damage to Reputation and Brand

Trust can be lost, particularly for consumer facing brands

Regulatory Issues

Regulators are facing pressure to punish breaches more severely. Rules are being tightened and penalties increased

Although the media often focuses on cyber attacks that lead to the theft or ransoming of customer data, there are many other types of potential risks. Among them are:

1 Business interruption

If a cyber adversary were to gain administrative control of OT systems that control building automation systems (BAS) or physical security management systems (PSMS), the results can be dangerous and costly. Fire alarms could be triggered, comfort systems could be disabled, or controls could be turned to uncomfortable or unsafe temperatures. The result can range from a temporary interruption of business to the destruction of a work product in a temperature controlled environment.

2 Higher insurance premiums

Overlooking BAS cybersecurity can also have insurance repercussions because actuaries are aware of the risk an organization faces when it is the victim of a targeted cyber attack. Insurance premiums will be higher if the organization cannot prove it has taken steps to strengthen its cyber resiliency. It is also likely that the insurance claim for the financial loss incurred will be denied.

3 Damage to reputation and brand

While other types of companies are not immune to the damage a cyber attack can impact reputation and brand, this problem is particularly true for consumer brands. For example, food and pharmaceutical manufacturing and storage facilities require a temperature-controlled environment. If temperature controls are compromised and cyber adversaries feed the facilities management team false data, products can spoil, pharmaceuticals can be rendered ineffective, consumer health can be impacted, and C-level executives can be held responsible for the fines incurred and the damage inflicted on brands and stock prices.

4 Regulatory issues

As new regulations for cybersecurity are issued, regulators across all industries are increasing the penalties on companies that are breached because they failed to take steps to adequately protect their businesses and the safety of their products. There is the potential for fines for regulatory non-compliance as well as remedial oversight by regulators.

8 http://www.aon.com/2017-global-risk-management-survey/

Damage to credit rating; M&A due diligence

Both Moody's and Standard & Poor's have publicly stated that suffering a cyber attack, or being inadequately prepared for a potential attack, can damage a company's credit rating. Cyber breaches are also becoming a factor in M&A due diligence.

Impact on key industries

Industry-specific examples provide further insight into the ramifications of cyber attacks:

Healthcare

Hospitals are a dynamic environment with multiple operational requirements within one site. Operating theatres, clean rooms, patient units, communal areas – all require different temperatures, lighting, and levels of security. Since cyber adversaries understand these facilities are high-value targets that can be coerced into paying a ransom, hospitals are vulnerable. The "Wannacry" ransomware attack on the UK's National Health Service in May 2017 showed what happens when hospitals are hit, including cancelled operations, ambulances being diverted, patient records made unavailable, and staff, patients, and equipment being in the wrong location.[9]

Premium office

Investment in the premium office space market is increasingly focused on solution offerings that improve employee welfare and boost operational efficiency. Company management usually views computers as the main cyber threat and attention is focused on ensuring that related software is up to date to prevent attacks. The challenge is that cyber adversaries often focus on weaknesses in support technology as a way in to causing wider disruption. Networked comfort systems or networked CCTV systems[10] are a prime example – they have a comparatively long lifetime compared to computers, and yet many are not updated or are secured with default passwords.

Life sciences

The June 2017 "NotPetya" ransomware attack on Merck, a leading global pharmaceutical company, led to a halt in drug production and research, lost sales, and other high-dollar expenses that totaled almost $600 million in losses over two quarters.[11] Although the attack came through the IT network, the OT network at life sciences companies are also important to protect in order to ensure a secure, controlled environment. A cyber-attack on a comfort system for a laboratory conducting controlled experiments that require specific atmospheric conditions could corrupt the data for an entire research project.

Data centers

Data centers are an attractive target for cyber adversaries because of the vital role they play in hosting business-critical systems for commerce and government. Due to their criticality, data centers have high levels of physical and cyber security, including multiple back-up provisions in case of a power failure. But the range of operational subsystems – including cooling systems, air handling units, motor controls, as well as back-up uninterruptible power supplies (UPS) and generators – means multiple points of potential vulnerability exist. Unfortunately, securing data center networks and servers counts for nothing if a UPS or cooling system is hacked and taken offline or instructed to operate in a sub-optimal manner.

Transportation

The volume of people using public transportation systems in large cities each day means that even a minor disruption can quickly become significant for tens or hundreds of thousands of people. Public transportation relies on surveillance cameras for security throughout the network, including stations. If a cyber breach occurred in a station's network it could jeopardize public security and hamper law enforcement efforts to keep the public safe, and the cameras themselves could be used for other nefarious purposes. For example, a well-publicized attack against several websites in September 2016 showed what could happen in the transportation industry when 1.5 million surveillance cameras were hijacked and used in a distributed denial of service (DDoS) attack.[12]

9 https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scalecyber-attack
10 https://www.youtube.com/watch?v=rZoslioj1zg&feature=youtu.be
11 https://www.techrepublic.com/article/notpetya-ransomware-outbreak-cost-merck-more-than-300m-per-quarter/
12 https://www.theguardian.com/technology/2016/oct/22/cyber-attack-hackers-weaponisedeveryday-devices-with-malware-to-mount-assault

Hospitality

Hotels have been investing substantial sums in improving the intelligence of their operations in order to drive operational efficiency. The large international corporates led the way, but advances in security and lighting technology, for example, are increasingly being adopted by small and medium sized hotel groups. In January 2017, the ransomware attack on the 4-star Romantik Seehotel Jaegerwirt in Austria crippled the hotel's ability to issue new key cards until the ransom was paid.[13]

Utilities

Utilities are a critical element of national infrastructure and require a high level of protection. The core power equipment within plants is one aspect and has its own protection, but the operational systems and equipment within control rooms and the overall site are also important. In December 2017, for example, cyber adversaries targeted an unnamed power plant, taking control of the safety control workstation.[14] Although this hack was defeated, it was one of many recent attacks focused on lower criticality systems designed to test power plant infrastructure and probe for weaknesses.

Oil and gas

Maintaining production in the oil and gas industry is critical; an unscheduled shutdown results in immediate financial losses for the company and damage to the local economy. The low oil prices of 2015 to 2017 forced oil and gas companies to tighten capital expenditures, but they have maintained their cybersecurity budgets, aware of the threats that exist in an industry that is increasing its use of cloud-based data solutions.

Airports

Security at airports has long been paramount, but it is the rise of automation that is ultimately changing the threat landscape. In March 2016, a Vietnamese man used the credentials of a third-party contractor to access the computer systems at Perth airport with the primary aim of stealing credit card data.[15] In the process he was able to steal building plans and details of physical security at airport buildings. However, he did not access systems linked to aircraft operations.

Domain knowledge is absolutely fundamental to the Siemens proposition. We know how your business operates, how your buildings work, and what needs to be done to make sure they are secure.

13 http://www.wired.co.uk/article/austria-hotel-ransomware-true-doors-lock-hackers
14 https://www.theguardian.com/technology/2017/dec/15/triton-hackers-malware-attack-safetysystems-energy-plant
15 https://thewest.com.au/news/wa/significant-amount-of-sensitive-security-data-stolen-in-perthairport-hacking-ng-b88686393z

Organizations cannot turn away from digital transformation initiatives, IoT, smart building systems, and the integration and communication between OT systems and IT systems. Neither can they continue to ignore the substantial business and financial risks they face when they curtail or fail to fund cybersecurity initiatives since they are just as important to business continuity and resiliency as accounting, finance, sales, marketing, and human resources departments. The challenge is to find the right strategy to minimize the threat of a cyber attack. But there are some common myths that get in the way for many organizations.

Exhibit 3 – Common Cyber Security Myths

1 "Purchase a Security Solution and Never Worry Again"

Nothing could be further from the truth. Cybersecurity is an ongoing process that requires collaboration between the C-level management team who proactively provides budget and support, facilities management teams who control OT systems, and IT teams who understand cybersecurity issues. A key step toward OT system cyber resiliency is the implementation of a hardened BAS or PSMS platform solution, but this is only part of the story. IT teams have an ongoing role to play in minimizing potential threats that can move laterally from IT systems to OT systems. IT systems must be promptly patched and adequately protected against unauthorized access. When they are not, and cyber adversaries breach the network, the BAS or PSMS platform can become a desirable target.

2 "Smaller Enterprises Need a Much Lower Level of Protection than Multinationals"

Business size is not the determining factor in deciding the level of protection required. Instead, companies need to understand the acceptable level of risk they are willing to take and the potential impact a business disruption resulting from an OT system compromise can create. If an enterprise of any size is operating in a high-risk business environment where a disruption could cause losses and place the viability of the business at risk, a higher priority should be placed on the cyber preparedness and resiliency of both OT and IT systems.

Continued operational vigilance is vital

Any enterprise is vulnerable and the impact of any attack is disproportionate to smaller organizations

Humans are a big part of the problem – also the solution

Operational criticality should be considered when deciding coverage

4 "People Are Largely Passive in the Cyber World"

The perception exists that people are largely passengers in the world of cyber security, but this is wrong. People are part of the problem and the solution. Every organization should closely examine its vulnerabilities in relation to human activity. For example, employees can unwittingly facilitate an attack by opening a link containing malware that creates a gateway into the wider network. Educating the workforce about cyber threats will turn employees into a security asset rather than a weakness.

3 "One Size Fits All Cybersecurity Solution for an Enterprise"

Believing that the level of cyber preparedness used for premium office space will work for data centers, manufacturing and processing facilities, laboratories, or refrigerated storage units is a recipe for business disruption and financial loss. Even within SMEs, the threat level and potential impact varies greatly depending on the operation.

Since the cyber threat landscape evolves daily, organizations must reconsider their thinking that cybersecurity is a once every two-to-three-year expenditure. Instead, cybersecurity initiatives must be proactively supported by the board of directors and funded with the understanding that the very survival of modern business requires cybersecurity to be a continuous process of year-over-year improvement that secures all aspects of the business.

Just because a business is small does not mean it will not be targeted – and for small businesses, the loss of intellectual property can be critical.

Best Practices: “Defense in Depth” and “Secure by Design”

“Know the enemy” is an important aspect of developing effective defenses against cyber threats. To that end, it must be acknowledged that cyber adversaries rarely devote 100% of their efforts to a single system. The typical approach is to view a business as a matrix of people, applications, networks, and processes with weaknesses in multiple places. Finding the way in through a chink in an organization’s security armor requires a variety of tools and techniques and a willingness to target multiple business departments. In response, you must take a “defense in depth” approach.

As a leader in the field, Siemens understands the full spectrum of security challenges organizations like yours are facing, from physical to cyber threats. You can provide the defense in depth that will protect your organization by taking the following three steps.

The first step involves general physical security – including physical access to the facility, organizational measures such as security policies, and monitoring the facility for anomalies that could indicate a cyber attack.

The second step, safeguarding networks, includes the installation of firewalls and the encryption of data transmission.

The third step focuses on system integrity – protecting the individual terminals and systems from access by unauthorized individuals as well as unauthorized changes.

As a result, potential attackers must overcome a combination of obstacles, which is much more difficult and time-consuming than simply cracking individual safety measures.

Cyber attacks are the reason we are committed to engineering secure products and solutions that can respond to a fast, complex, and ever-changing threat landscape. We take a “secure by design” approach that integrates cradle-to-grave activities. By adhering to the main pillars of prevention, detection, and reaction, we are continuously developing our products, solutions, and services.

Cyber attacks are the reason Siemens is committed to engineering secure products.

Our organizational focus on secure product engineering is evangelized by our CEO and has had a profound impact on organizational culture and processes.

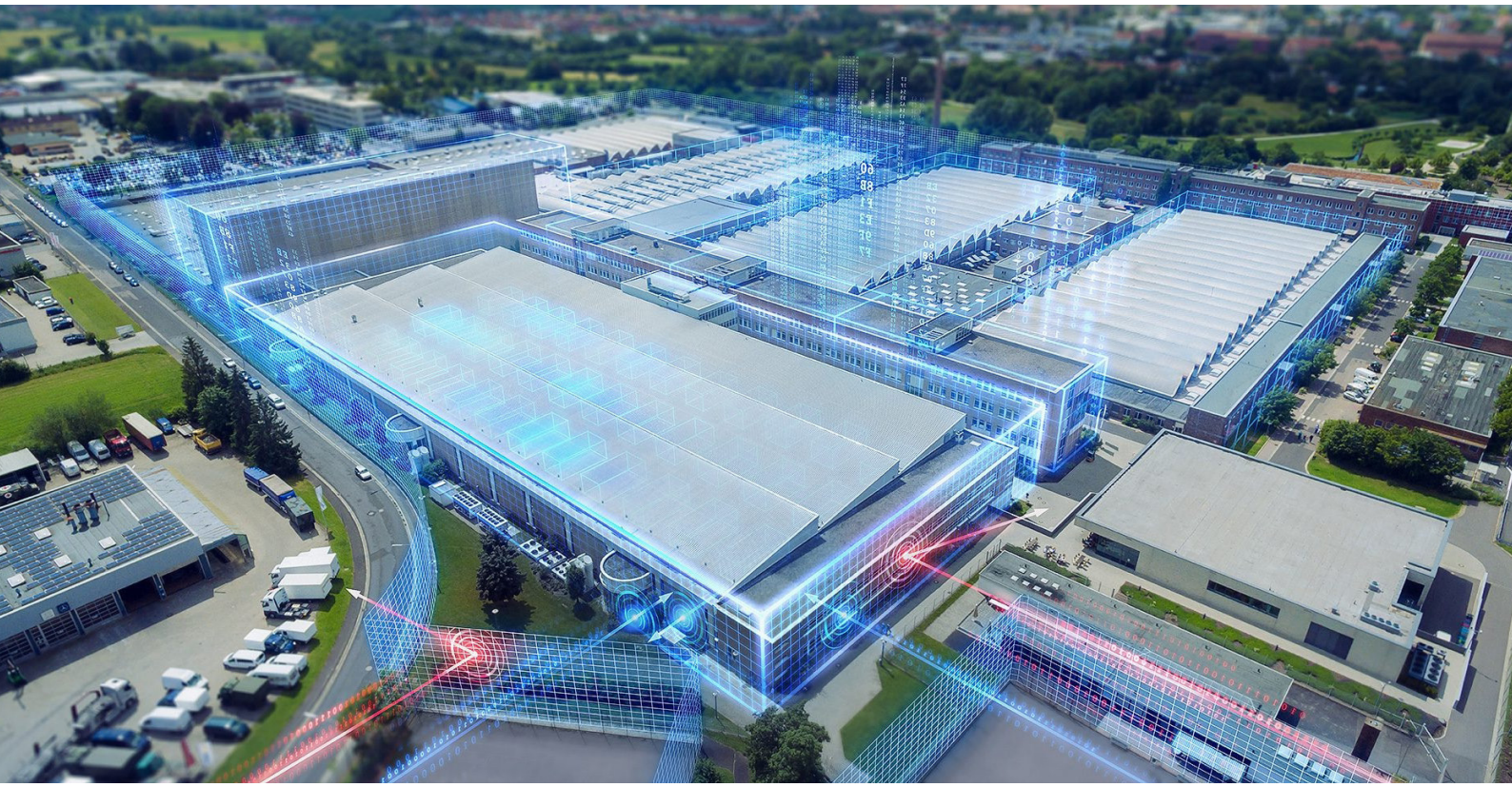
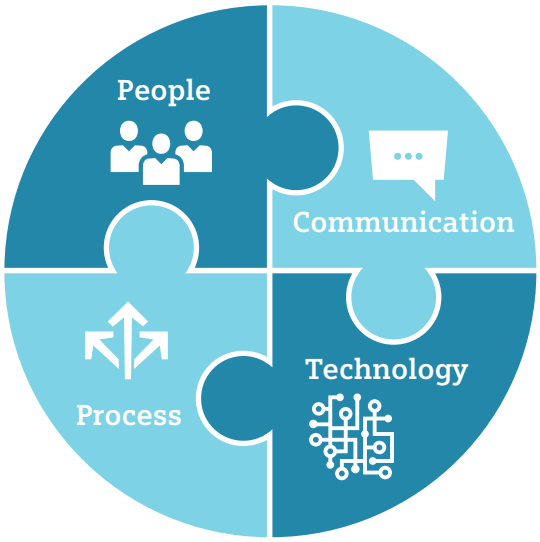


Exhibit 4 – Siemens' Cybersecurity Model

Siemens' Cybersecurity Model adds another layer to defense in depth by taking into account four key factors: **People, communication, process, and technology.**



1 The People Factor

Ensuring a broad and lasting awareness of the importance of security is a key component of the Siemens security model that is woven into product development and processes.

2 The Communication Factor

Clear, consistent, and friction-free communication helps establish a culture of security among the people in an organization.

3 The Process Factor

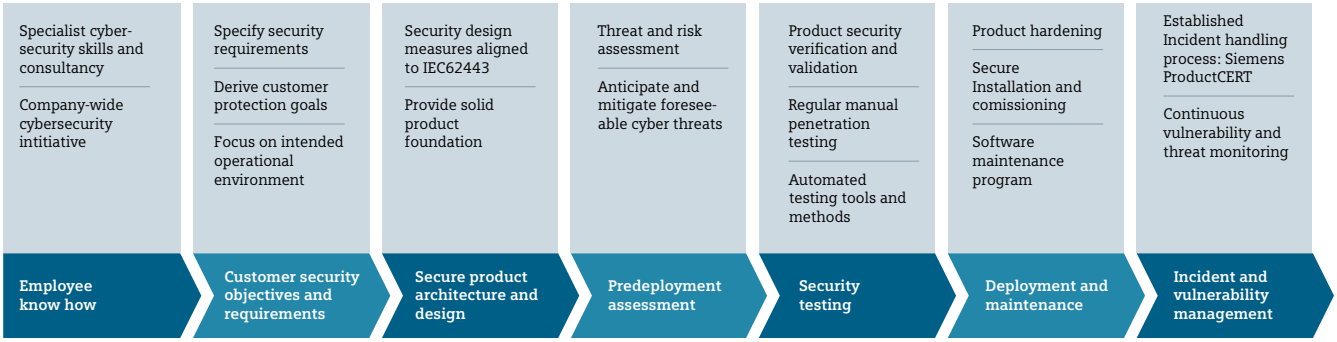
Organizational processes are just as important to security as the technology that is used to protect a company from cyber threats.

4 The Technology Factor

Knowing which security technologies and building blocks are suitable for a given organization is important.

Understanding the details around these four factors allows us to recommend the appropriate security tools for different business needs. The Siemens approach to security is outlined in exhibit 5.

Exhibit 5 – Highlights of Siemens' Approach to Security



Frost & Sullivan's Security Maturity Model

In 2017, Frost & Sullivan conducted research into the overall security preparedness of large UK enterprises to determine how organizations think they are doing compared to what they are actually doing.[16] The research led to the development of the Frost & Sullivan Security Maturity Model[17] and the five security axes that when analyzed together provide an objective look at an organization's preparedness. The five axes are:

1 Organization culture

Focuses on the culture of the entire organization instead of the individual and is frequently described as "how we do things around here." It examines the degree to which an organization has integrated information security into its day-to-day operation.

2 Technology tools and controls

Examines the extent to which the organization has advanced its security processes.

3 Security operations

Measures the extent to which security guidelines have been developed and formally put in place across the organization.

4 People

Measures the training and organizational dedication to implementing security assurances across all departments at the individual level.

5 Cloud adoption

Measures the progress and security around an organization's adoption of cloud-based services.

16 https://www.secureworks.co.uk/resources/at-a-new-security-maturity-model-how-does-yourbusiness-stack-up
17 Jarad Carleton and Jason Reed. "Measuring Cybersecurity Preparedness: Illuminating Perception versus Reality in UK Enterprise." Frost & Sullivan Paper, 2017

Based on these axes, benchmarks were developed that allowed further analysis of the surveyed organizations. Frost & Sullivan found that companies fall into three distinct groups on the security maturity continuum that ranges from low to high maturity.

The groups were named:

1 Underprepared –
Organizations in this category exhibit the following:

- Low or non-existent levels of staffing charged with information security responsibilities
- Few formal security guidelines outside of the IT department
- Lower adoption rates of security tools and controls

2 In transition – Have the following:

- Demonstrated understanding of need for personnel that are charged with handling information security
- Some have implemented formal guidelines for all departments, however some have not
- Some have semi-automated their security practices, however most have not or have yet to implement the tools, controls, and operational procedures to provide top-tier protection

3 Security leaders – Do the following:

- Have implemented best practices for organizational preparedness, have fully briefed all employees on security protocols and incident response action plan
- Continuously test security architecture to ensure maximum functionality
- Despite this, many still are not proactively anticipating unknown threats, indicating that even leaders in the field have room for improvement

Even organizations categorized as security leaders have potential chinks in their cybersecurity armor.

There are two key findings from the Frost & Sullivan research that cannot be ignored. First, 52% of the surveyed organizations fall into the "underprepared" category. Second, many of the 27% that are considered "security leaders" still have potential chinks in their cybersecurity armor that can by leveraged to gain unauthorized access to networks as well as critical business and building systems.

Perception vs. Reality

Differences between how secure an organization believes itself to be and the reality of its security maturity are frequently out of alignment. Perception versus reality misalignment occurs when an organization does not establish well defined and measurable key performance indicators (KPIs) that enable it to track progress, stagnation, or regression on the security maturity model continuum. These KPIs must not be confused with ones used to measure productivity, which does not equate to security maturity. In the absence of a set of meaningful security KPIs, an organization is left guessing about the actual state of its security program.

Business Resilience Requires Cyber Resilience

Far too frequently organizations do not include cyber resilience in their business continuity discussions.[18] However, without a proactive cybersecurity strategy that includes automated building systems as well as business applications and networks, it is not possible to ensure an organization will have the resilience to overcome the unexpected with minimal disruption to productivity and revenues. In fact, without a coherent cybersecurity strategy, a security incident in IT can rapidly cascade across the business, causing substantial disruption in unexpected areas, including the ability to utilize offices with networked physical access systems, fire alarms, lighting, and controls.

18 https://www.citrix.com/articles/7-key-elements-of-business-continuity.htmlvey/

Exhibit 6 – Elements of Business Resilience Impacted by a Cybersecurity Incident

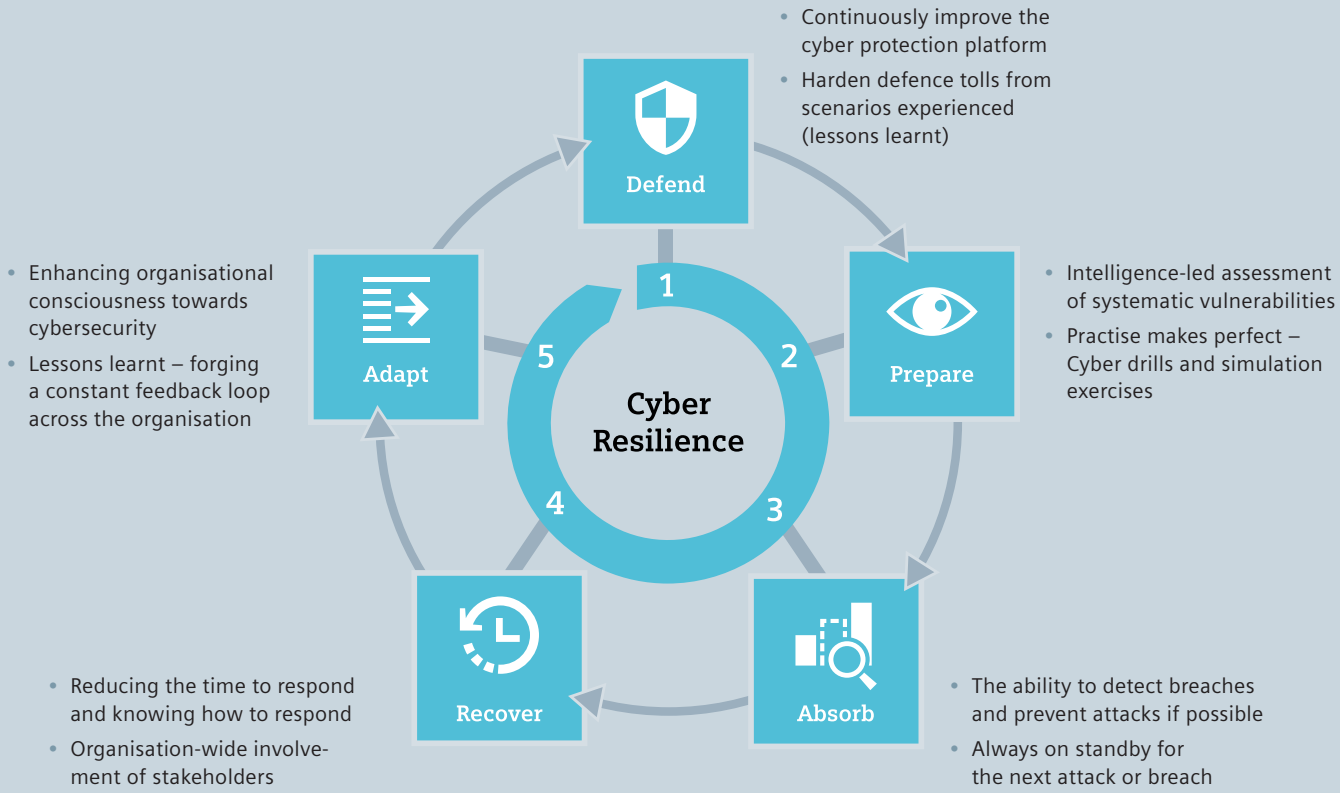
Source: Frost & Sullivan and Citrix

Attaining Cyber Resiliency

Cyber resiliency is attainable, but only when executives acknowledge that it takes a commitment to year-over-year improvement that cannot be abandoned when it becomes inconvenient. The commitment starts with the board of directors and C-level executives and is subsequently pushed across the entire business. Frost & Sullivan's five-step Cyber Resilience Framework illustrates the initiatives that must be incorporated into an organization's culture in order to improve its security maturity score year-over-year. Without such a commitment, the organization might not survive the real cyber threats to enterprises that are occurring in the digitized global marketplace.

Becoming cyber resilient requires a systemic commitment that starts with the board of directors and C-level executives and is subsequently pushed across the entire business.

Exhibit 7 – Frost & Sullivan
5-Step Cyber Resilience Model



Source: Frost & Sullivan

Siemens' approach to cyber resiliency adopts and integrates proven security models. Attaining cyber resiliency requires every organization, including Siemens and its customers, to have processes that clearly map back to the security best practices discussed here. It is this type of focus on continuous improvement that is needed to ensure the security of building systems that are connected to networks.

Siemens' approach to cyber resiliency has been built into the process factor of our security model.

Conclusion

Digitalization delivers significant benefits and opportunities, but it must be pursued hand in hand with cybersecurity in order to combat the types of threats discussed in this paper. Knowing where your organization falls on the Frost & Sullivan security maturity continuum is a good first step. It helps you know the real state of your security program so you can identify any gaps.

If you have not already done so, the second step is to adopt a proven security model, one with best practices, processes, and KPIs. Commitment needs to start at the top, with the board of directors and C-level executives leading the charge. Since cybersecurity relies on engagement across the entire organization, investment in additional people, technology, or processes may be required. It may also be necessary to revamp recruiting tactics to make sure you have people with the right skills who can implement and manage your security strategies.

Avoiding common myths about cybersecurity is an important step three. The size of the company does not determine the level of protection required and security is not a one and done investment. Regular reviews are necessary to help you keep pace with the evolution of cyber threats. In addition, cybersecurity needs to be part of your business continuity planning. The increasingly interconnected nature of business calls for you to look beyond your own operations and consider the possibility of threats to your supply chain and third-party vendors. Who would be responsible in such a breach? How easy would it be to trace the origin of a breach? Prevention is more effective than trying to counteract the impact of a breach once it has occurred.

The fourth step involves the convergence of OT and IT. Although they have been viewed separately in the past, it is advantageous to monitor them using a single dashboard. This will give you better insight into your strengths and weaknesses across the board. Our long-term commitment to OT cybersecurity puts Siemens in the unique position of being able to offer this capability through Desigo CC and Siveillance solutions.

Finally – don't get carried away by the media hype. Cyber threats are real, but the right actions can mitigate and defend against them. Deferring investment in new technology and solutions that can drive business resiliency is a far greater threat than taking the precautions necessary to minimize the risks of a cyber breach.

Link to Siveillance WP – https://www.hqs.sbt.siemens.com/hqcc/step-assets/Whitepaper_cybersecurity_EN.pdf
Link to Siemens AG Cybersecurity page – https://www.siemens.com/global/en/home/company/topic-areas/digitalization/cybersecurity.html
https://www.siemens.com/global/en/home/company/topicareas/digitalization/cybersecurity.html
https://www.siemens.com/global/en/home/company/innovation/pictures-of-thefuture/cybersecurity.html

Published by
Siemens Switzerland Ltd 2018

Building Technologies Division
International Headquarters
Gubelstrasse 22
6301 Zug
Switzerland
Tel +41 41 724 24 24

Status 07/2018