Cybersecurity Trends 2018

Perspectives on cybersecurity in an increasingly digital world.

www.tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.

Content

Dear Readers,

As predicted in our last year's report, the past months saw a dramatic increase in the volume, sophistication and persistence of cyberattacks. It was a year when nothing seemed safe, and where cyberattacks illuminated the vulnerability of our personal data.

In April, an anonymous group called the Shadow Brokers leaked a suite of hacking tools suspected to belong to the US National Security Agency. In July, attackers stole the personal data of 145 million people from Equifax. WannaCry and NotPetya ransomware outbreaks followed and spread to over 150 countries, contributing to suggested ransomware payments exceeding $2 billion in 2017, and FedEx attributing a $300 million loss to the NotPetya attack alone. Both of these, now infamous, ransomware attacks exploited the vulnerability leaked by the Shadow Brokers. Most recently, revelations of harvesting of user profiles from Facebook has highlighted the far-reaching risks that stem from the misuse of our most personal information. It now seems easier than ever to create malware, or ransomware, or gain access to personal data. So as businesses continue on their digital transformation journeys and we continue to integrate 'smart' devices into our daily lives, cybercrime increasingly represents a major threat to society.

In this year's report, we focus on where we see the most significant threats and also some opportunities emerging. We highlight the implications of our increasingly connected world, how global regulation is responding, the need to inject trust into cybersecurity, ways to protect ourselves from 'intelligent' cyberattacks, and what we should do to close the skills gap in an environment starved for cybersecurity talent, yet overwhelmed by volumes of data.

We hope you find it engaging and insightful, and look forward to continuing the dialogue with you on these topics.

FRANK LUZSICZA, EXECUTIVE VICE PRESIDENT,
ICT & BUSINESS SOLUTIONS, TÜV RHEINLAND GROUP

Executive Summary

Perspectives on cybersecurity in an increasingly digital world.

What challenges do organisations have to face in the next months, what threats should they be prepared for?

TREND 1: A RISING GLOBAL TIDE OF CYBER-REGULATION INCREASING THE PRICE OF PRIVACY

Data protection is a critical concern in an increasingly digital world and May 25, 2018 is a turning point for data protection in Europe. It marks the end of the transitional period for the EU General Data Protection Regulation (GDPR) as it becomes enforceable by law. It disrupts data governance and how information is protected for any organisation controlling or processing EU citizen personal data, and leads a growing list of emerging data protection regulations from around the globe. Failure to comply could result in fines of up to 4% of global turnover – a significant sum that demands attention. Expect to see the EU Commission hold major global companies accountable for GDPR violations.

TREND 2: THE INTERNET OF THINGS DRIVES THE CONVERGENCE OF SAFETY, CYBERSECURITY, AND DATA PRIVACY

In 2016, Mirai proved that Internet of Things (IoT) devices can be effectively weaponised as botnets. Today, product development, time to market considerations, and technical power constraints leave IoT devices exposed by exploitation of critical vulnerabilities. The impact of data breaches now extends far beyond simple data monetisation to 'kinetic' threats to health and safety, as devices and systems are directly connected to open networks. It is widely accepted that the state of IoT security is poor and, with over 500 connected devices expected to cohabit with us in our homes by 2022, these represent a major risk to safety, cybersecurity, and data privacy.

TREND 3: OPERATIONAL TECHNOLOGY EMERGES AS A FRONTLINE FOR CYBERATTACKS

The industrial internet is already transforming global industry and infrastructure, promising greater efficiency, productivity and safety. To compete means to move process equipment online, often unwittingly exposing component vulnerabilities to cyberattacks. Manufacturing plants are targeted to obtain intellectual property, trade secrets, and engineering information. Attacks on public infrastructure are motivated by financial gain, hacktivism, and national state agendas. Fear of a 'worst-case scenario', where attackers trigger a breakdown in systems that underpin society, was highlighted this year at the World Economic Forum. Industrial systems are particularly susceptible to supply-chain attacks, adversaries have recognised this and are targeting them.

TREND 4: WITH CYBER DEFENCES IN PLACE, FOCUS SHIFTS TO THREAT DETECTION AND RESPONSE

Recent cyberattacks on high-profile organisations are proving that, against the sophisticated and persistent cybercriminals, preventative controls alone are not enough. Today, it takes organisations, on average, over 191 days to detect a data breach. The longer it takes to detect and respond to threats the greater the financial and reputational damage done to the organisation by the incident. Due to the vast growth of security log data, limitations of incumbent technologies, ineffective use of threat intelligence, inability to monitor IoT devices, and shortage of cybersecurity talent, organisations are exposed to costly dwell times.

TREND 5: INCREASING USE OF ARTIFICIAL INTELLIGENCE FOR CYBERATTACKS AND CYBER DEFENCE

As organisations undergo a digital transformation, there is a growing volume of increasingly sophisticated and persistent cyberattacks. Malware is becoming smarter, able to 'intelligently' adapt to and evade traditional detection and eradication measures. With a global shortage of cybersecurity talent, organisations are losing the cyber arms race as a result. The volume of security data now far exceeds our legacy capability to use it effectively, leading to a growing number of AI-enabled cybersecurity use cases: accelerating incident detection and response; better identifying and communicating risks to the business; providing a unified view of security status across the organisation.

TREND 6: CERTIFICATIONS BECOME NECESSARY TO INJECT TRUST INTO CYBERSECURITY

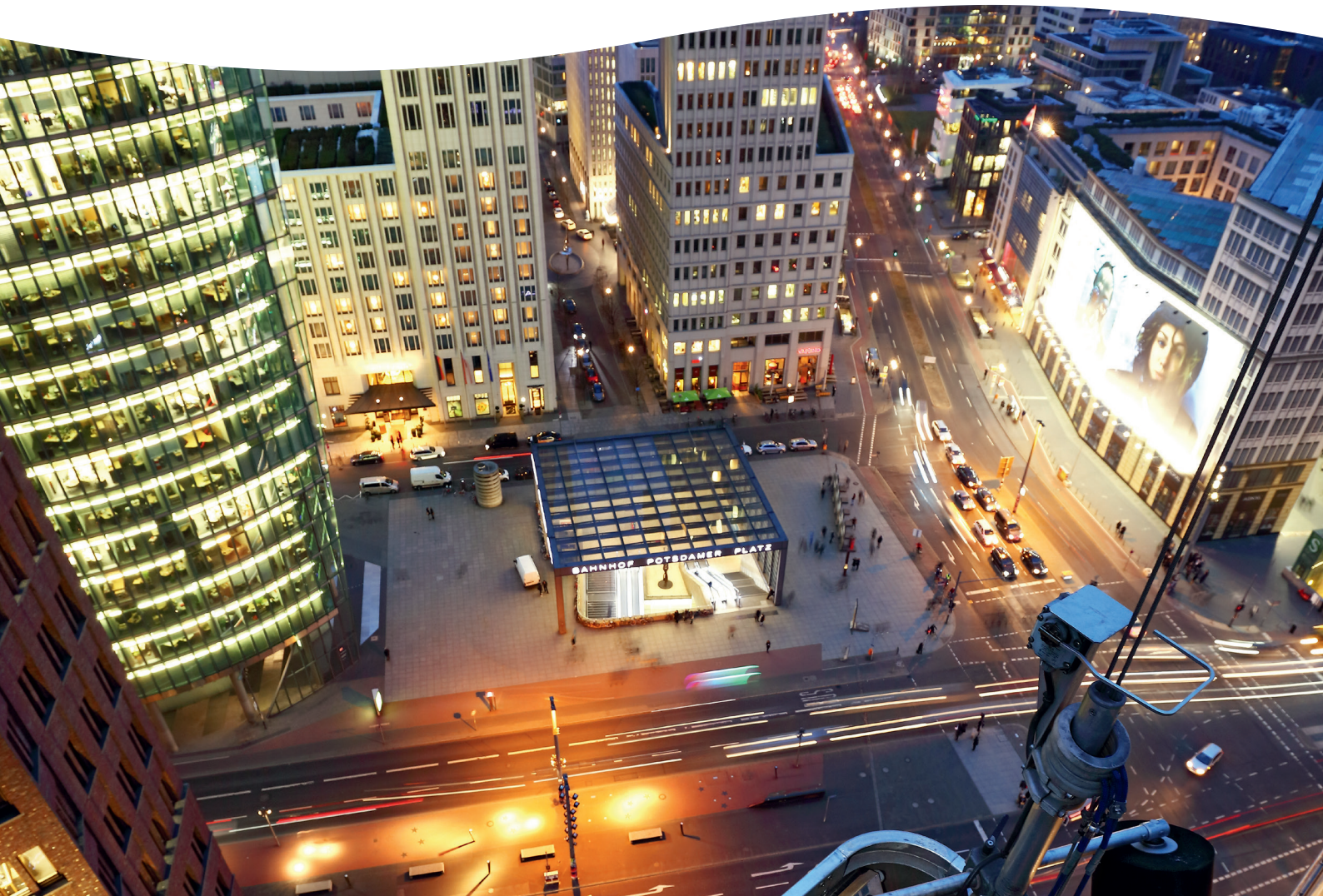
It is broadly accepted that cybersecurity and data protection are of critical importance in an increasingly digital world, but how can you judge the effectiveness of an organisation's cybersecurity posture? There is a growing concern for trust in cybersecurity, evidenced by existing and emerging standards. For CISOs and product manufacturers alike, certification validates you have done what you say you have done. Today, however, product security assurance certification schemes tend to focus on the critical infrastructure and government sectors only. Where does that leave the manufacturers of consumer products?

TREND 7: PASSWORDS BEING REPLACED BY BIOMETRIC AUTHENTICATION

Our digital lives are ruled by a complex web of online apps each requiring a username and password to control access. To protect the data behind these apps, selecting an obscure and complex password, and changing it often, is good practice, but also quite rare. With exponential improvements in computing power, and easy access to lots of it in the cloud, the time it takes to brute force passwords is rapidly reducing. What took nearly 4 years in 2000, now takes only 2 months. Add to that the fact stolen, hacked and traded passwords have never before been so openly available. As a result, it is increasingly commonplace to encounter biometric authentication (facial, fingerprint, iris, and voice) included in everyday mobile, tablet, and laptop devices, as well as physical access and online services.

TREND 8: INDUSTRIES UNDER SIEGE: HEALTHCARE, FINANCE, AND ENERGY

The majority of cyberattacks are undertaken by criminal organisations and are motivated by money. The value of information on the dark web depends on demand for the data, the available supply, its completeness, and ability for reuse. As a result, healthcare and financial personal information are highly sought after. Medical records can fetch $1-$1,000, depending on how complete they are, while credit cards can fetch only $5-$30 dollars, if bundled with the information necessary to do immediate damage. Other cyberattacks have more political and nation-state motives, here disruption to critical services through attacks on the energy sector is a key risk in 2018; as evidenced by recent news of Russia's campaign of cyberattacks targeting the U.S. power grid, which is suspected to have been underway for several years.



Trend 1: A rising global tide of cyber-regulation increasing the price of privacy

Data protection is a critical concern in an increasingly digital world and May 25, 2018 is a turning point for data protection in Europe. It marks the end of the transitional period for the EU General Data Protection Regulation (GDPR) as it becomes enforceable by law. It disrupts data governance and how information is protected for any organisation controlling or processing EU citizen personal data, and leads a growing list of emerging data protection regulations from around the globe. Failure to comply could result in fines of up to 4% of global turnover[1] — a significant sum that demands attention. Expect to see the EU Commission hold major global companies accountable for GDPR violations.

1 European Commission, May 2017

"The GDPR is a challenge for companies, but also an opportunity to optimize data governance and related protection measures to reduce the risk of data protection breaches."

MICHAEL SILVAN,
Chief Technology Officer (CTO),
Center of Excellence
Risk & Compliance,
TÜV Rheinland

DATA PROTECTION IS A CRITICAL CONCERN IN AN INCREASINGLY DIGITAL WORLD

As business undergoes digital transformation and becomes increasingly connected, cyberattacks continue to grow in both sophistication and volume. Recent high-profile cyberattacks have showed us just how vulnerable organisations are. The ransomware WannaCry infected more than 300,000 computers across multiple organisations, countries, and continents in less than 48 hours. 87 million Facebook profiles harvested by political consultancy Cambridge Analytica is being dubbed one of the most consequential data breaches in history, rivalling the breach of financial records from Equifax. These attacks predict a dark future for privacy.

GDPR DISRUPTS THE DATA GOVERNANCE AND HOW INFORMATION SHOULD BE PROTECTED

Increasingly, organisations must be able to prove that they are processing personal data in accordance with the legal requirements of this evolving regulatory environment. GDPR introduces a number of key components including: Extra-territorial reach over EU data; Individual right; Data privacy officers; Notice and consent; Restrictions on secondary users; Privacy impact assessment; and Data breach notification. These requirements are forcing organisations to rethink data governance, systems architecture, documentation, and data loss prevention.

FAILURE TO COMPLY COULD RESULT IN FINES OF UP TO 4% OF GLOBAL TURNOVER

The related business risk is material. In the event of non-compliance or contravention, the EU is envisioning sanctions amounting to four percent of the previous year's turnover, or EUR 20m, whichever is the greater. Weaknesses in technical and organisational data security, such as outdated encryption standards, leave organisations vulnerable to these fines.

MANY ORGANISATIONS ARE UNDERESTIMATING THE EXTENT OF SUCH REQUIREMENTS

Few organisations are going to be ready by the impending deadline. Most, having underestimated the extent of the requirements, are still developing their plan for GDPR compliance. Some have decided not to develop a plan, choosing instead to treat non-conformity as just another operational risk to be managed – perhaps doubting the seriousness with which the EU commission will enforce it. Others are not sure if the regulation applies. As a result, the majority of organisations are starting late with implementation.

AN EMERGING LIST OF DATA PROTECTION REGULATIONS FROM AROUND THE GLOBE

GDPR is leading a global trend as European regulators are not alone in mandating greater accountability at the executive level. The USA, Argentina, Brazil, Switzerland, Africa, India, and China are all revising their data protection regulations. Many share similar concepts, like informed user consent and data breach notification obliging organisations to notify the relevant authority and all affected data subjects when a breach occurs; an often costly exercise. Yet this also leads to fragmentation and emerging market barriers driven by territorial requirements for data protection and data flows across borders. For global organisations, this will make international operations an increasingly costly and complex challenge.

www.tuv.com/data-privacy-management

Trend 2: The Internet of Things drives the convergence of safety, cybersecurity and data privacy

In 2016, Mirai proved that Internet of Things (IoT) devices can be effectively weaponised as botnets. Today, product development, time to market considerations, and technical power constraints leave IoT devices exposed by exploitation of critical vulnerabilities. The impact of data breaches now extends far beyond simple data monetisation to 'kinetic' threats to health and safety, as devices and systems are directly connected to open networks. It is widely accepted that the state of IoT security is poor and, with over 500 connected devices expected to cohabit with us in our homes by 2022, these represent a major risk to safety, cybersecurity, and data privacy.

MIRAI PROVED THAT IOT DEVICES CAN BE EFFECTIVELY WEAPONISED AS BOTNETS

At 7am ET Friday, October 21, 2016 a massive Distributed Denial of Service (DDoS) attack hit Dyn Inc. and temporarily disrupted much of the internet on the East Coast of the United States. It affected companies like Twitter, Spotify, Amazon, Netflix, Reddit, the Guardian, CNN, and the New York Times. Formed mainly of hacked IoT devices, the Mirai botnet was a wake-up call about the vulnerability of internet connected 'things' to cyberattacks.

COMMERCIAL AND TECHNICAL CONSTRAINTS LEAVE IOT DEVICES VULNERABLE TO EXPLOITS

Many IoT devices are fundamentally insecure, leaving product manufacturers and customers exposed to the inherent risk of cyberattacks. This should not come as a surprise as manufacturers are not in the business of cybersecurity. Instead, they are under increasing pressure to innovate faster than the competition, while protecting their margins. Ensuring devices are easy to produce, functional, connected, and secure – while limiting power consumption to extend battery life – is a complex technical challenge leading to difficult trade-offs.

VULNERABILITIES OFTEN RESIDE DEEP IN THE PRODUCT SOFTWARE STACK

To save time and money, software developers use open source code libraries; rather than reinvent the wheel for basic features. These 3rd party libraries can be a source of critical vulnerabilities. A good example is the Devil's Ivy vulnerability, recently found in the gSOAP toolkit that is often used by manufacturers to connect their devices to the internet. It is estimated that over one million devices exist that are vulnerable to the Devil's Ivy stack buffer overflow exploit.

> "Only if manufacturers identify the threats and risks linked with their device and address suitable consequences for privacy during design, they can focus on their product innovations and improved market opportunities."

UDO SCALLA,
Head of Competence Center IoT Privacy, TÜV Rheinland

THE IMPACT OF DATA BREACHES NOW EXTENDS FAR BEYOND SIMPLE DATA MONETISATION

We are increasingly living in one integrated digital system aimed at improving the quality of our lives. But consumers simply do not have the knowledge to protect themselves from these vulnerable IoT ecosystems. Product manufacturers who neglect cybersecurity and data privacy concerns are delivering their customers into the hands of cybercriminals. In a world of cyber-physical things, this is a threat to personal health and safety, not just personal information.

HACKABLE MEDICAL DEVICES ENDANGER PATIENT LIVES

Last year, the FDA confirmed that St. Jude Medical's implantable cardiac devices, including pacemakers and defibrillators, were vulnerable to cyberattacks. Attackers could gain control of devices via accessing the transmitter that reads device data and sends it back to physicians. Another example is that of a baby heart monitor where an unencrypted Wi-Fi network between the monitor and sensor left it vulnerable to cyberattack. Attackers could take control of the system and monitor a stranger's baby and stop alerts being sent to the parents[2].

HACKABLE CARS LEAVE PASSENGERS AT THE MERCY OF THEIR ATTACKERS

In 2015, a team of researchers was able to take complete control over a Jeep SUV. The vehicle's CAN bus was hijacked over the cellular network by exploiting a firmware update vulnerability. The researchers were able to remotely speed up, slow down, and even steer the vehicle off the road. More recently, it was reported that a new vulnerability in CAN protocol that is not only nearly universal, but can be exploited while bypassing the auto-industry's attempts at cybersecurity controls[3]. It allows attackers to shut off critical safety and security systems including airbags, anti-lock brakes, and door locks. It represents a vulnerability in the design of the CAN standard itself.

Common products go online and join the Internet of Things

www.tuv.com/en/iot-privacy

2 The Register, Wi-Fi baby heart monitor may have the worst IoT security of 2016, October 2016
3 Wired, Car hack shut down safety features, August 2017

Trend 3: Operational Technology emerges as a frontline for cyberattacks

The industrial internet is already transforming global industry and infrastructure, promising greater efficiency, productivity and safety. To compete means to move process equipment online, often unwittingly exposing component vulnerabilities to cyberattacks. Manufacturing plants are targeted to obtain intellectual property, trade secrets, and engineering information. Attacks on public infrastructure are motivated by financial gain, hacktivism, and national state agendas. Fear of a 'worst-case scenario', where attackers trigger a breakdown in systems that underpin society, was highlighted this year at the World Economic Forum. Industrial systems are particularly susceptible to supply-chain attacks, adversaries have recognised this and are targeting them.

THE INDUSTRIAL INTERNET IS TRANSFORMING GLOBAL INDUSTRY AND INFRASTRUCTURE

For the past 15 years, the internet has been transforming the business to consumer relationship, democratising information-based industries such as media, retail, and financial services. For the next 10 years, it is set to disrupt physical industries manufacturing, energy, transportation, and agriculture. Dubbed the 'Industrial Internet', the trend to integrate information and operational technology networks will bring unprecedented opportunities along with new risks.

"The ability to assess, detect, monitor and manage cybersecurity threats in Operational Technology will play a vital role in determining the safety and resilience of Industrial plant operations."

URMEZ RUSI DAVER,
Leader, Center of Excellence Industrial Security,
TÜV Rheinland

TO COMPETE MEANS TO MOVE PROCESS EQUIPMENT ONLINE

For decades, measurement data has been used by industrial sectors to improve productivity and competitiveness, and to save energy. At its most basic level, current data is compared to historical data to determine how processes should be run. Analytics provide recommendations, enhancements, and warnings to support decision making[4]. The next big step for industrial evolution is to move measurement data outside of the facility and into the Cloud. This way information from process equipment from all over the globe can be combined, leading to new opportunities for competitive advantage.

FEAR OF A 'WORST-CASE SCENARIO' IS HIGHLIGHTED BY THE WORLD ECONOMIC FORUM

The volume and sophistication of cyberattacks is escalating, having almost doubled over the past 5 years. Historically, industrial systems were standalone and not connected to corporate networks or the internet, but in an increasingly connected industrial world, cybercriminals now have exponentially greater number of potential targets. As a result, there is a growing trend to attack critical and strategic infrastructure across the world, including government, railways, banks, telecommunications, energy, manufacturing, and hospitals; raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the systems that keep society functioning.

MANUFACTURING PLANTS ARE TARGETED TO OBTAIN TRADE SECRETS

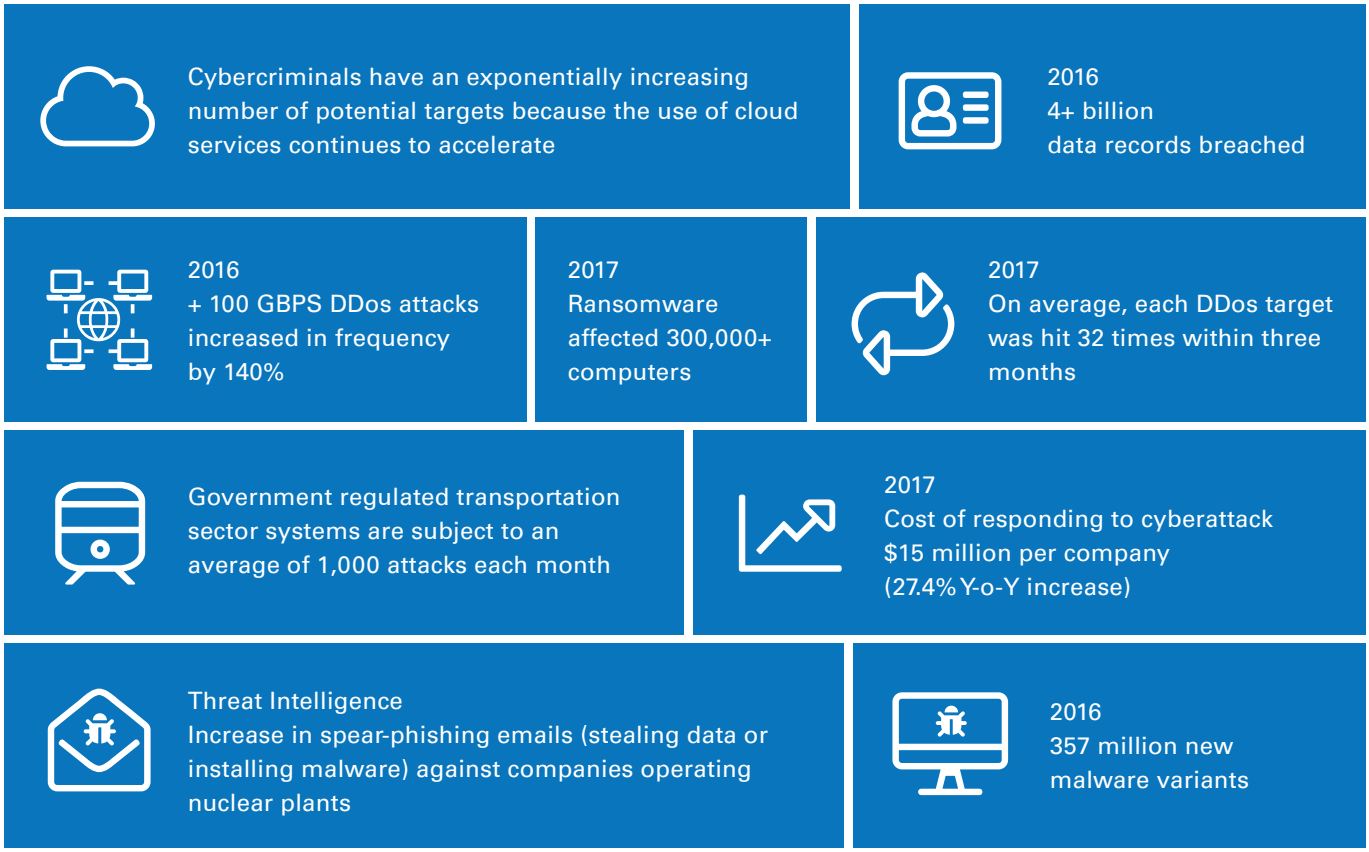
As the volume of cyberattacks increases, manufacturing is becoming one of the most targeted industries. Just over a third of documented cyberattacks are targeting the manufacturing industry, with manufacturers appearing in the top three targets in five out of six geographies[5]. This is because of the fierce competition in a sector where intellectual property is at a premium, yet investment in cybersecurity is lacking due to commercial focus on productivity and efficiency.

PUBLIC INFRASTRUCTURE ATTACKS HAVE DESTRUCTIVE MOTIVES

Often overshadowed by the sheer scale of personal information being stolen by cybercriminals in the enterprise sector, cyber espionage groups are continuing to escalate their access to public infrastructure across the globe[6]. For the past decade destructive attacks have been increasingly targeting a variety of organisations and critical infrastructure, but with a definite 'spike' in the past 18 months. The 'Crash Override' malware was used to attack the Ukraine power grid and was able to take control of grid circuit switches and breakers. More recently, attackers breached nuclear plants in order to map out computer networks and process control systems for future attacks.

4 ABB, The Internet of Things, Services and People – A new age of industrial production, 2016
5 Computerweekly, Manufacturing a key target for cyberattacks, August 2017
6 Business Insider Germany, Destructive cyberattacks are only going to get worse, September 2017

Global cyberthreat trends for Operational Technology



TARGETING OF SUPPLY CHAINS IS AN EMERGING THREAT

Industrial processes depend on a regular supply of resources and logistical support. Attackers have recognised the importance of supply chains and have started targeting them with interception, infiltration, counterfeit and disruption. This can be demonstrated by the impact of cyberattacks on the global logistics industry. Last year, FedEx and AP Moller-Maersk reported combined business losses of nearly $600m after being hit by Ransomware and 'Wiper` virus attacks. As supply chains become more global, the risks from intentional insertion of malicious functionality increases.

ADDITIONAL BUDGETS ARE REQUIRED TO ADDRESS RISING COMPLIANCE REQUIREMENTS

In this context, organisations will need to allocate additional budgets to detection technologies and incident response; as opposed to prevention technologies only. Artificial Intelligence (AI) and predictive analytics for cyber risk management of Operational Technology will be adopted. Compliance requirements from regulators to secure critical infrastructure will rise and increase the cost of compliance for Operators. Regional and industry specific standards will bring clarity to the compliance regimen. Privacy regulations like GDPR will find its way into this domain where Operators will be faced with a unique set of challenges around managing data protection and privacy especially with IIOT (Industrial Internet of Things).

www.tuv.com/en/industrial-sec

Learn more about Industrial Security in our global report, coming in July 2018.

Stay tuned:
www.tuv.com/en/OT

Trend 4: With cyber defences in place, focus shifts to threat detection and response

Recent cyberattacks on high-profile organisations are proving that, against the sophisticated and persistent cybercriminals, preventative controls alone are not enough. Today, it takes organisations, on average, over 191 days to detect a data breach. The longer it takes to detect and respond to threats the greater the financial and reputational damage done to the organisation by the incident. Due to the vast growth of security log data, limitations of incumbent technologies, ineffective use of threat intelligence, inability to monitor IoT devices, and shortage of cybersecurity talent, organisations are exposed to costly dwell times.

ORGANISATIONS CONTINUE TO TAKE TOO LONG TO DETECT A DATA BREACH

The faster a data breach can be detected and contained, the lower the costs and impact on reputation and business value. It takes a cybercriminal a matter of minutes to hours to compromise a network and extract basic data, or days to weeks to identify and steal critical data. Yet, organisations take on average 191 days to detect a breach and 66 days to contain it. Organisations who can get their detection time below 100 days can save over $1m. Furthermore, when a data breach is disclosed, stock price declines immediately by an average of five percent in line with customer confidence. For those organisations that demonstrate rapid detection and response times, stock price rebounds quickly; but for the rest, it often never fully recovers.

TRADITIONAL APPROACHES TO THREAT DETECTION ARE CUMBERSOME

Traditional approaches are built around Security Information and Event Management (SIEM) solutions. Unlike security cameras that go straight from installation to insight, traditional SIEM solutions are plagued with painful implementation, limited scalability, difficulty in integrating data sources, and convoluted reporting process – they take a small army of security analysts to figure out. This is exacerbated by the fact that the amount of data analysed by security teams is doubling each year, and shifting towards unstructured; a data type traditional SIEM tools are not able to analyze.

THE MAIN CONCERNS OF TÜV RHEINLAND EXPERTS:

- "... insecure IoT devices that nobody updates and have full access to the internet."
- "... the protection of critical national infrastructure and risks to public safety and national economy."
- "... the lack of proactive investment. Currently, money is usually spent following a cybersecurity incident or if there is a regulatory requirement."
- "... inadequate cybersecurity awareness on employee and management level."
- "... safety risks ignored driven by emphasis on data confidentiality. Family technology solutions that expose elderly or children to cyberattacks."
- "... missing budget for cybersecurity initiatives."
- "... cybersecurity skill and resource shortage."

THE CYBERSECURITY SKILLS SHORTAGE IS GETTING WORSE

IT organisations continue to cite cybersecurity as the biggest area where they have a problematic skills shortage. Looking back through the ESG's annual global survey on the state of IT shows an alarming growth of the issue, more than doubling from 23% of organisations in 2014 to 51% in 2018[7]. It is expected that there will be 3.5 million unfilled cybersecurity jobs by 2021. More than half-million of these are predicted to emerge in the U.S. The cybersecurity skills shortage is getting worse and there is no evidence to suggest it will slow down in the foreseeable future.

RAPID CYBERTHREAT DETECTION AND ACCURATE RESPONSE REQUIRES A NEW APPROACH

Modern malware and sophisticated cyberthreats require a proactive, agile approach to replace traditional SIEM solutions. Traditional solutions work to detect known threats within fixed enterprise network perimeters using signature-based techniques that are no longer effective. To materially reduce detection times and accelerate containment, organisations will increasingly adopt advanced security analytics. This new approach uses machine data to identify anomalies from a pre-determined baseline of usage behaviour across the dynamic landscape of the modern Digital Enterprise.

BARRIERS TO EFFECTIVE USE OF THREAT INTELLIGENCE REMAIN

In an environment of 'big security data', the combination of advanced threat intelligence, and a team of security analysts can lead to actionable insight. Threat intelligence is not a technology, it is the knowledge about adversaries, their means, motives, and intentions. It should be disseminated in a way that supports cybersecurity teams and the business to protect the critical assets of the enterprise. Yet, even the most cutting-edge threat intelligence is ineffective if you do not have the people with the knowledge, skills and experience to do something with it. Unfortunately, there is a huge skills gap across the industry such that only the most attractive brands with the largest budgets, at the top of the market, will be able to acquire and retain the necessary talent.

www.tuv.com/en/apt

7 CSO online, research suggests cybersecurity skills shortage is getting worse, January 2018

BRIAN NOLAN,
Chief Technology Officer (CTO), Center of Excellence Advanced Threat, TÜV Rheinland

"2018 will be a pivotal year for companies to adopt new approaches to threat detection. We will help our customers utilize new cloud-native security analytics and machine learning technologies to analyze the vast amount of security logs and data, better leverage threat intelligence, monitor IoT and OT technologies, and cope with the shortage of qualified cybersecurity personnel."

Trend 5: Increasing use of Artificial Intelligence for cyberattacks and cyber defence

As organisations undergo a digital transformation, there is a growing volume of increasingly sophisticated and persistent cyberattacks. Malware is becoming smarter, able to 'intelligently' adapt to and evade traditional detection and eradication measures. With a global shortage of cyber-security talent, organisations are losing the cyber arms race as a result. The volume of security data now far exceeds our legacy capability to use it effectively, leading to a growing number of AI-enabled cybersecurity use cases: accelerating incident detection and response; better identifying and communicating risks to the business; providing a unified view of security status across the organisation.

ORGANISATIONS ARE LOSING THE CYBER ARMS RACE

Gone are the days when cyberattackers were little more than annoying 'script-kiddies', they have graduated to well-funded organised-cybercrime, and nation-state actors. They are a legitimate and sophisticated threat that regularly disrupt organisations and governments alike. Cybercrime is very lucrative, low risk, and global. And, it is not as if the cybersecurity industry is standing still, yet the attackers can keep winning; so by leaving vulnerabilities unpatched, we are making it too easy.

NIGEL STANLEY,
Chief Technology Officer (CTO), Center of Excellence Industrial Security, TÜV Rheinland

"Cyber Threat Intelligence (CTI) is vital and threat hunting can only work well if it has a good intelligence feed. But only a few people understand both cybersecurity and intelligence gathering to an expert level."

FOR EXPERTS OF TÜV RHEINLAND, THREAT INTELLIGENCE IS A STRATEGIC BUSINESS-TO-BUSINESS COLLABORATION TOOL AND AN IMPORTANT MEANS OF SHARING KNOWLEDGE BETWEEN ORGANISATIONS ...

1. .... to detect incidents more effectively.
2. .... to react to incidents more quickly and more efficiently.
3. .... to strengthen their own strategic role when responding to cybersecurity events.

THE VOLUME OF SECURITY DATA NOW FAR EXCEEDS OUR LEGACY CAPABILITY TO USE IT

Most large organisations have deployed, and potentially integrated, dozens of security technologies. The digital economy is connecting everything to everything else, leading to billions of new endpoint devices. As a result, we are generating so much security event log and alert information, that it is no longer possible to see the forest from the trees. This is making the job of protecting the organisation increasingly difficult, and perhaps represents an even greater risk than the escalating sophistication of cyberattacks themselves.

THE ERA OF AI POWERED CYBERATTACKS HAS STARTED

AI threatens to exacerbate the already considerable cybersecurity challenge faced by organisations in an increasingly digital world. They are rare today, but we are seeing signs of AI-based advanced cyberattacks. Last year, we witnessed the first artificial intelligence based cyberattack, where rudimentary machine learning was used to study patterns of normal behaviour within a company's networks[8]. Once a baseline was established, the malware then began to mimic normal network behaviour to become almost undetectable.

CYBERSECURITY LEADERS WILL DEFEND AGAINST AI ATTACKS BY USING AI

The next-generation of cyberattacks will use AI-based malware capable of reacting in real-time to evade cybersecurity controls and necessitate new defensive approaches. Cybersecurity professionals are looking towards advanced cyber defences which use AI to proactively respond to such attacks. On a good day, human security analysts alerted to a potential phishing attack can contain the incident in a matter of hours. AI-based security automation can detect and contain the same incident within minutes. It is, therefore, increasingly considered a critical component in a modern cybersecurity strategy.

TURNING TO AI PLUGS THE GROWING SHORTAGE OF CYBERSECURITY TALENT

Using AI security teams can quickly make sense of massive amounts of security data, putting alert information and event logs into far greater context. This ability to prioritise and focus on the highest risk threats holds great promise for organisations trying to protect their critical assets with scarce cybersecurity resources. This will, however, lead to some defensive roles (Tier 1 and Tier 2 security analysts, or security operations centre [SOC] analysts) to be at risk of being replaced by AI in the next 5-10 years[9].

www.tuv.com/en/pentest

8 Wall Street Journal, The Morning Download: First AI-Powered Cyberattacks Are Detected, November 2017
9 Security Now, Ai is stealing these IT-Security-Jobs now, March 2018

Trend 6: Certifications become necessary to inject trust into cybersecurity

It is broadly accepted that cybersecurity and data protection are of critical importance in an increasingly digital world, but how can you judge the effectiveness of an organisation's cybersecurity posture? There is a growing concern for trust in cybersecurity, evidenced by existing and emerging standards. For CISOs and product manufacturers alike, certification validates you have done what you say you have done. Today, however, product security assurance certification schemes tend to focus on the critical infrastructure and government sectors only. Where does that leave the manufacturers of consumer products?

EFFECTIVE CYBERSECURITY IS NEEDED FOR A VIABLE IOT-BASED DIGITAL ECONOMY

With a growing share of services offered online, and the rapid proliferation of connected devices, it is increasingly apparent that cybersecurity plays a critical role in the viability of our digital economy. Protecting our digital ecosystems, from critical infrastructure to consumer devices must be a fundamental requirement for doing digital business. As a result, cyberthreats pose a serious risk to the fabric of contemporary society[10].

LEADING TO A GROWING CONCERN FOR TRUST IN CYBERSECURITY

In fact, this year's World Economic Forum Global Risks Report states that cyberattacks against businesses have doubled over the last five years. And so this year saw a significant jump in concern over cyberattacks and massive data fraud, with both ranking in the top five global risks by perceived likelihood[11]. A Pew Research Center survey found that the majority (64%) of Americans have personally experienced a major data breach, and that many do not trust modern organisations to protect their personal information[12]. The European Commission announced two initiatives related to certification and labelling: a security framework for ICT (Information and communications technology) products, and a 'Trusted IoT label' giving information about different levels of privacy, security and, where relevant, demonstrating compliance with The Directive on security of network and information systems (NIS Directive); adopted by the European Parliament in 2016.

IMPACTING THE BUSINESS ECOSYSTEMS AND SUPPLY CHAINS

The ongoing digital transformation of business is leading to increasingly complex and networked ecosystems and supply chains, with the automotive industry being a good example. Here, the Trusted Information Security Assessment Exchange (TISAX) audit is gaining traction. TISAX enables accredited providers to offer mutually accepted assessments based on the VDA (German Association of the Automotive Industry) Information Security Assessment; which, in turn, is based on a catalogue of information security criteria incorporating key aspects of international ISO/IEC 27001 and 27002 standards.

10 DIGITALEUROPE's views on Cybersecurity Certification and Labelling Schemes, March 2017
11 World Economic Forum: The Global Risks Report 2018, 13th Edition
12 Pew Research Center, Americans and Cybersecurity, January 2017

"A certification signals a high level of IT security according to national or international standards. This creates comparability on the market and confidence – if the certification framework is transparent and clear."

DR. DANIEL HAMBURG,
Leader, Center of Excellence
Testing and Certification,
TÜV Rheinland

CERTIFICATION VALIDATES YOU HAVE DONE WHAT YOU SAY YOU HAVE DONE

With cybersecurity acknowledged to be of such critical importance, a key question becomes how can you judge the effectiveness of an organisation's cybersecurity posture? The existence of corresponding certification plays an important role, for example in making a decision on whether to impose administrative fines and on their amount. A certification procedure can prove that the provisions of a new regulation have been observed and implemented in full.

REGULATED CERTIFICATION SCHEMES LAG THE MARKET NEED

The concept of a security certification framework for products and services is a good one, but these should be done at a global level, if at all possible, and in such a way not to give a false sense of total security. National level schemes, for example, that define standards and evaluation methods, and only recognise certification bodies within their own territory would create market inefficiencies. Recent experience with Common Criteria has shown that even if a pan-region approach is achieved, global support is required to avoid multiple regional certifications for one product. In the end, cybersecurity is a global issue and requires international solutions.

CONSUMERS NEED EASY TO UNDERSTAND TRANSPARENT INFORMATION

Independent product evaluation can be a very resource-intensive process, and so tends to focus on high risk government or critical infrastructure products and services. This gives rise to process-based approaches including ISO/IEC 27034, as well as certifications for specific types of systems such as ISA/IEC 62443. But with pressure for even faster, cheaper product development lifecycles, agile assessment schemes, utilizing test automation environments will need to be created and evolved.

www.tuv.com/en/data-privacy-certification

Trend 7: Passwords being replaced by biometric authentication

Our digital lives are ruled by a complex web of online apps each requiring a username and password to control access. To protect the data behind these apps, selecting an obscure and complex password, and changing it often, is good practice, but also quite rare. With exponential improvements in computing power, and easy access to lots of it in the cloud, the time it takes to brute force passwords is rapidly reducing. What took nearly 4 years in 2000, now takes only 2 months. Add to that the fact stolen, hacked and traded passwords have never before been so openly available. As a result, it is increasingly commonplace to encounter biometric authentication (facial, fingerprint, iris, and voice) included in everyday mobile, tablet, and laptop devices, as well as physical access and online services.

PASSWORD BEST PRACTICE IS WELL KNOWN, BUT FRUSTRATING TO FOLLOW

Traditional best practice approaches to creating passwords has made us lazy. Making use of irregular capitalisation, special characters, and numbers, then being forced to change it every 90 days lead to passwords like 'P@ssW0rd123!'. Such passwords are hard to remember but relatively easy to guess. When faced with logging into an application after an extended period of time, it is frustrating to reset your password because you have forgotten it. The issue is that most people tend to use the same techniques when crafting passwords that leave them predictably vulnerable to password cracking algorithms that target those specific weaknesses.

MOORE'S LAW RENDERS PASSWORDS WEAKER OVER TIME

Over time passwords weaken dramatically as computing power doubles every 18 months, and cybercriminals become more proficient. For example, a password that would take over three years to crack in 2000 takes just over a year in 2004, and five years later in 2009 just 4 months. In the modern era, passwords simply do not stand up against sophisticated cyberthreats. A third of cybercrime originates from stolen passwords, and over 1.5 billion passwords have been stolen.

MARK CODERRE,
Leader, Center of Excellence Risk & Compliance, TÜV Rheinland

"Adaptive, risk-based authentication solutions will become more common. But the future of authentication has already begun."

13 Better Buys, Estimating password cracking times

EXPERTS OF TÜV RHEINLAND FORESEE USER IDENTIFICATION IN NEW METHODS:

- **Certificate-based authentication** or mutual authentication. This describes a process in which two parties (mostly a client and a server) mutually authenticate one another. Use of a digital certificate enables the user, computer or the device to be identified before they are granted access to a resource, a network, an application, etc.
- **Biometric recognition** which is now being offered by device manufacturers and which works by using the unique human characteristics to prove the identity, may be the key to a much more effective system. Experts predict "an almost certainty" that within the next few years, three biometric options will become standard features in every new phone: a fingerprint scanner built into the screen, facial recognition powered by high-definition cameras, and voice recognition based on a large collection of a human vocal sample.
- **FIDO (Fast Identity Online)** is a set of platform-independent security specifications in order to facilitate strong authentication. The specifications for FIDO support MFA (multi-factor authentication) and cryptography with a public key. One major advantage of FIDO-compatible authentication is the fact that users do not have to utilize their complicated passwords. Nor do they have to cope with complex guidelines for strong passwords. If a user has forgotten his/her password, no resetting procedure is necessary. Unlike databases for passwords, FIDO stores personal identifying information (PII), e.g. biometric authentication locally, i.e. on the user's device in order to protect it adequately.

AN EMERGING THEME FROM RECENT DATA BREACHES POINTS THE FINGER SQUARELY AT PASSWORDS

In many of the recent headline-grabbing data breaches, the attack vector has been a common password[14]. This is not surprising given how many people reuse passwords between accounts. For example, the breach of a White House contractor was made possible by him reusing the same password as his Gmail account; which turned out to have been stolen during the Adobe breach in 2013. In fact, as many as two-thirds of data breach incidents are a result of leveraging weak, stolen, or default passwords. And nearly all phishing attacks are after user credentials[15].

BIOMETRIC AUTHENTICATION DETERMINES EXACTLY WHO IS ACCESSING A SYSTEM

Biometric authentication creates accountability; every access or action is recorded along with the individual associated with it. This naturally reduces the risk of misuse, fraud, and data leakage. Within the next few years, three biometric options will become standard features in every new phone: a fingerprint scanner built into the screen, facial recognition powered by high-definition cameras, and voice recognition based on a large collection of a human vocal sample. The number of fingerprint reader-equipped devices has already passed a billion[16]. Unlike passwords, there is no way for someone to forget his or her biometric credentials, and this information is very difficult to forge. On the downside, if the biometric credentials are ever compromised, it is very difficult to alter one´s fingerprint or their appearance.

www.tuv.com/en/iam

14 CNBC, Passwords are the weakest link in cybersecurity today, October 2016
15 IDAgent, 63% of Data Breaches Result From Weak or Stolen Passwords, 2016
16 Information Age, In the modern era biometrics should replace passwords, February 2017

Trend 8: Industries under siege: Healthcare, Finance, and Energy

The majority of cyberattacks are undertaken by criminal organisations and are motivated by money. The value of information on the dark web depends on demand for the data, the available supply, its completeness, and ability for reuse. As a result, healthcare and financial personal information are highly sought after. Medical records can fetch $1-$1,000, depending on how complete they are, while credit cards can fetch only $5-$30 dollars, if bundled with the information necessary to do immediate damage. Other cyberattacks have more political and nation-state motives, here disruption to critical services through attacks on the energy sector is a key risk in 2018; as evidenced by recent news of Russia's campaign of cyberattacks targeting the U.S. power grid[17], which is suspected to have been underway for several years.

MEDICAL INDUSTRY: VERSATILE CHALLENGES – GROWING SPENDING

In 2017, cyberattacks struck hospitals and health systems at an alarming rate[18] and the cybersecurity exposure is still growing: With the increase in the digitalization and use of healthcare information, the availability of consumer access to private health information (PHI), continued innovation and availability of consumer-focused health applications and devices as well as the growth of networked medical devices, the cyber exposure in the healthcare industry will rise. The challenges of cybersecurity in the healthcare sector are also versatile. Whether it is malware that compromises the integrity of systems and privacy of patients or Distributed Denial of Service (DDoS) attacks that disrupt facilities' ability to provide patient care: Cyberattacks can have other results than only financial loss or the breach of privacy – the direct impact on human lives. Patient safety, financial loss, disruption of health services, reputation damage, and exposure to litigation related to cyberattacks remain the key risks for the medical industry in 2018.

The consequence: Organisations spend more to protect their systems and patient data. Cybersecurity Ventures predicts global healthcare cybersecurity spending will exceed $65 billion cumulatively over the next five years, from 2017 to 2021[19].

17 Reuters, In a first, U.S. blames Russia for cyberattacks on energy grid, March 2018
18 Health IT & CIO Report, 11 of the biggest healthcare cyberattacks of 2017, December 2017
19 CSO online, Why healthcare cybersecurity spending will exceed $65B over the next 5 years, February 2018

FINANCIAL SECTOR: INCREASED VOLUME AND COMPLEXITY OF ATTACKS

The area of financial services is relatively well-developed in terms of cybersecurity. This is also largely due to legal regulations, for example in regard to risk management. Nevertheless, 2017 was a game changer: We saw an increased volume and complexity of cyberattacks due to the growth of cybercrime services in which advanced attack capabilities are sold to and leveraged by less sophisticated adversaries. Reported cyberattacks against financial services firms rose by 80 percent in the last year, reflecting the increasing number of attacks aimed at organisations[20]. And the risk of cyberattacks is being amplified by the significant outsourcing done by investment dealers and asset managers[21].

DIFFERENT ATTACK VECTORS — ONE GOAL: MONEY

Different cybercriminal groups penetrated bank infrastructures, e-money systems, cryptocurrency exchanges, capital management funds, and even casinos, in order to withdraw large sums of money. In this context, the interception of bank customers' electronic operations through the hijacking of bank domains in order to perform phishing attacks, install malicious code and wield the operations of customers who were using online banking services at the time appear already traditional.

The main key events were continuous cyberattacks targeting systems running SWIFT[22], which affected several banks in more than 10 countries around the world. In addition to the SWIFT attacks, cybercriminals have been actively using ATM infections, including those on financial institution's own networks and PoS terminal networks[23], to change card balances. Attacks on ATMs became so popular in 2017, that the first ATM malware-as-a-service was offered.

NEW UNKNOWN RISKS AS A RESULT OF OPEN BANKS ECO-SYSTEMS

In the future, it is expected that the financial sector will suffer further financial losses, interruptions in critical services and the risk of legal disputes in connection with cyberattacks due to DDoS attacks and financial malware, as an example. New as yet unknown risks will also arise as a result of the demand for further opening up of banks´ eco-systems.

Moreover, significant reputational damage is expected for financial organisations, when banks and insurers are forced to reveal any data breaches that occur in the context of the GDPR. The customer trust in banks and insurers still remains high, with 82 percent rating them among the most trusted institutions, maybe due to the practice that financial organisations fail to voluntarily share news of data security breaches[24].

The great cybersecurity opportunity for financial organisations will be to cooperate and co-ordinate across the financial sector, involving insurance, banking and security firms, pointing in the right direction, because cybersecurity in the context of critical infrastructures is a task for the whole society.

20 Information age, Rise cyberattacks financial services firms, January 2018
21 Financial Post, Financial firm outsourcing increasing risk of cyberattacks: IIAC, January 2018
22 Financial Post, Financial firm outsourcing increasing risk of cyberattacks: IIAC, November 2017
23 Point of Sale Terminalnetwork
24 Computerweekly, Finance firms are vulnerable to cyberattacks, so why do customers think they are secure?, February 2017

ENERGY SECTOR: ATTRACTIVE TARGET DUE TO ITS NATIONAL AND ECONONOMIC IMPORTANCE

The energy sector will be the prime target for cyber-attacks. Particulary, at risk are companies engaged in Alternative Energy Development, Coal Mining, Nuclear Energy Development, Natural Gas Distribution, Oil and Gas Exploration and Production, Oil and Gas Field Equipment Manufacturing as well as Oil and Gas Field Services Petroleum Refining. They are very interesting targets particularly given the importance to national and economic security. So it is no wonder, that concerns over potential cyberattacks on energy infrastructure have become increasingly pressing over the last year.

NEW QUALITY OF ATTACKS

In the limelight: "classical" data stolen from energy companies includes business process information, contract negotiations information, executive communication, market analysis and proprietary technologies[25]. In 2017, Dragonfly was synonymous with a new wave of cyberattacks that could provide attackers with the means to severely disrupt affected operations[26]. But the nature of attacks is changing: According to sources of the New York Times, hackers compromised computer systems at a petrochemical plant in Saudi Arabia in August 2017, aiming to not only destroy or steal data but to cause a deadly explosion – a new quality of an attack that could be replicated in other countries because the compromised systems are used in thousands of industrial plants worldwide[27].One of the recent events was the fact that in April 2018 the energy industry of the UK was on alert for cyberattacks on UK power network[28].
In this context, more and more governments worldwide are considering ways to optimise the police protection of critical infrastructure, such as nuclear sites. A regulatory framework for cybersecurity in critical sectors is due to be implemented by May 2018 in the UK.

SERIOUS IMPACT ON GENERAL SUPPLY SECURITY

The cybersecurity risks will grow: A decentralized energy supply system requires a distribution network which is no longer only based on conventional perimeter security. Smart grids represent a large number of gateways for advanced persistent threats and DDoS attacks. Increasing pairing of mobile private devices with low perimeter security involves considerable malware risks, e.g. in the case of WannaCry, which may also have serious impacts on the common good and general supply security.

25 Intelligence Report, Cyber threats to the energy industry, 2016
26 Symantec, Dragonfly: Western energy sector targeted by sophisticated attack group, October 2017
27 Oilprice, energy sector under threat from deadly cyberattacks, March 2018
28 Financial Times, energy sector on alert for cyberattacks on UK power network, April 2018

"Good cybersecurity hygiene will mitigate many of the risks. The problem is: We struggle with even the basics."

ANTHONY DICKINSON,
Head of Center of Excellence & Business Officer Strategy, TÜV Rheinland

www.tuv.com/informationsecurity

TÜV Rheinland
ICT & Business Solutions
cybersecurity@tuv.com

www.tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.