



Cybersecurity Trends 2019

New thinking on cybersecurity and privacy in
a world where digital transformation beckons.

www.tuv.com/informationsecurity

 **TÜVRheinland®**
Precisely Right.

Contents

03	Welcome Note
04	Executive Summary
06	Trend 1: Cybersecurity has become a board-level issue
09	Trend 2: Industrial cybersecurity is years behind mainstream IT security
11	Trend 3: IoT cybersecurity faces a major standards challenge
13	Trend 4: The pressure created by GDPR represents a turning point for consumer privacy
15	Trend 5: The cybersecurity skills shortage will distort the labor market
18	Trend 6: Threat detection and response depends on maturing Security Orchestration, Automation, and Response (SOAR)
20	Trend 7: 'Red team' testing and agile security development are gaining greater mainstream acceptance
22	Trend 8: Cybersecurity will define digital economy winners and losers

Dear Readers,

Following the publication of our Cybersecurity Trends report last year, 2018 proved to be another challenging year for everyone involved with cybersecurity. Although none of last year's incidents had as much public visibility, or widespread and devastating effects as the WannaCry and NotPetya attacks of 2017, numerous smaller incidents reminded us that cybersecurity and data privacy remain a critical undertaking.

In the early part of the year, we followed closely a new class of attack vectors, in the form of the 'Meltdown' and 'Spectre' security flaws, that lie deep in the architecture of many modern microprocessors and could take years to resolve. Soon after, we watched the very public ransomware extortion attacks on the city of Atlanta and the ports of San Diego and Barcelona; an alarming sign that cybercriminals are capable of targeting the critical infrastructure that our economies depend upon.

Another theme of 2018 was the continuing erosion of our data privacy. This was underscored by high-profile examples such as the Cambridge Analytica data scandal that enveloped Facebook, the data breach affecting 500 million customers at Marriot International, and the large volume of personal data stolen from German politicians and celebrities and then leaked earlier this year. The recent discovery of vast caches of stolen data, called Collections #1 - #5, demonstrates that cybercriminals have successfully combined thousands of smaller and forgotten data breaches into larger, more meaningful, databases.

These events represent a historic challenge for organizations investing in Digital Transformation and Industry 4.0 that even the much welcome arrival of the EU's General Data Protection Regulation (GDPR) in May 2018 is unable to fully address.

In this year's report, we explore how the evolution of cybercrime is affecting target-rich environments such as Operational Technology (OT) in industry, the Internet of Things (IoT), as well as the impact of the ongoing cybersecurity skills shortage and the balance of power across senior management functions. We also anticipate the increasing maturity of evolving concepts such as red team penetration testing, agile security, security automation, machine learning and big data analytics.



Sometimes, the challenges may seem overwhelming, but what matters far more is our ability to face these issues head on. At TÜV Rheinland, we firmly believe that with long-term dedication to innovation and investment in developing expertise, coupled with our unwavering commitment to client success, significant progress can be made.

A handwritten signature in black ink that reads "Frank Luzsicza".

**FRANK LUZSICZA, EXECUTIVE VICE PRESIDENT
DIGITAL TRANSFORMATION & CYBERSECURITY, TÜV RHEINLAND GROUP**

Executive Summary

New thinking on cybersecurity and privacy in a world where digital transformation beckons.

TREND 1: CYBERSECURITY HAS BECOME A BOARD-LEVEL ISSUE

Until recently, cybersecurity was viewed as an IT challenge rather than a business risk. Despite years of warnings, it took until the aftermath of the NotPetya cyberattack in 2017 to change this view. Several large companies announced huge losses arising from the incident, including shipping giant Maersk, FedEx, advertising company WPP, and home products company Reckitt Benckiser. All reportedly lost up to hundreds of millions each, making this the most expensive cyberattack in history. Meanwhile, data breaches continue to be a major cause for worry. Suddenly, cybersecurity has gone from being a hypothetical problem to an acknowledged business risk. This realization is now driving long-term changes in how cybersecurity risk should be managed, and by whom.

TREND 2: INDUSTRIAL CYBERSECURITY IS YEARS BEHIND MAINSTREAM IT SECURITY

An OT system is one where a computer controls or detects a physical action, which might be an electrical motor, a valve, or from a relay that has some sort of kinetic effect. For too long protecting these often safety-critical systems used by utilities such as energy, water and industry has been cybersecurity's poor relation, which has allowed complacency and under-investment to take hold. These days, new technology and geo-political tensions have fundamentally changed the risks of failing to protect OT, especially systems used to monitor safety. If something can be targeted, and at some point we must now assume it will be, we should do everything reasonable to avoid it being successful.

TREND 3: IOT CYBERSECURITY FACES A MAJOR STANDARDS CHALLENGE

Across the globe, standards bodies and industrial sectors are busily drafting the security and privacy standards necessary to secure the next wave of development in the IoT and OT. While the intention is good, this might result in a lot of confusion and wasted time as manufacturers attempt to work out which of these regional and sector-specific efforts they should comply with. Particularly at risk are global businesses that depend on having an understandable path to compliance to smooth their product development. As competing standards vie for importance, time could be wasted.

TREND 4: THE PRESSURE CREATED BY GDPR REPRESENTS A TURNING POINT FOR CONSUMER PRIVACY

Within months of the European General Data Protection Regulation (GDPR) coming into force in May 2018, the first trickle of prosecutions became public, including €50,000,000 fine imposed by the French data protection authority CNIL on a major search engine operator for not "clearly and comprehensibly" informing its users about the use of their personal data. Although this represents a slow start and the early fines have been modest in size, it is becoming clear that the GDPR will be a major influence on privacy across the whole world and not only in the EU itself. For most industries, it will simply be cheaper to design their products and services to conform to the highest global standards rather than geographically-defined privacy.

TREND 5: THE CYBERSECURITY SKILLS SHORTAGE WILL DISTORT THE LABOR MARKET

The surge in the importance of cybersecurity has come at a time when the skills required to strengthen it are in critically short supply. By 2020, globally this could reach 1.5 million, with some estimates putting the figure at more than double this by 2021. Under such an extreme skills shortage, market distortions start to occur, with larger, wealthier organizations and service providers able to attract talent while smaller companies in some sectors struggle. Inevitably, this not only makes cybersecurity more expensive but impacts supply chains that tie the economy of large and smaller companies together. For the long-term interests of the emerging industrial economy, cybersecurity is a common good that should be accessible to all. Failure to address this problem is to store up problems for the future.

TREND 6: THREAT DETECTION AND RESPONSE DEPENDS ON MATURING SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR)

Security Orchestration, Automation, and Response (SOAR) has huge potential to reduce the time to detect and respond to incidents and minimize the impact of cyberattacks. The biggest benefit may be automated containment workflows, which are critical when dealing with fast-spreading destructive malware. Other benefits include standardizing investigation processes, accelerating prioritization and response, enabling proactive threat hunting, and improving the quality and efficiency of detection and response processes.

However, implementing a new wave of automation requires investment and planning from organizations during a period when established investments such as Security Information and Event Management (SIEM) are still bedding in.

TREND 7: 'RED TEAM' TESTING AND AGILE SECURITY DEVELOPMENT ARE GAINING GREATER MAINSTREAM ACCEPTANCE

From its origins in the penetration-testing sector, red team or 'holistic' testing is the trend to simulate how an attacker might penetrate an organization under real-world conditions by exploiting any available weakness to gain access to a resource. While flaws can be found in many resources – applications, devices or infrastructure – red teams also look at broader issues such as social engineering, hijacking a social media presence, physical access to a building or, in the most challenging cases, malicious insiders. Unlike traditional pen-testing, red teaming tries to understand how these operate together rather than as a series of separate layers. Working in tandem with this is the rise of agile security testing, which aims to remove as many software vulnerabilities as possible during the development cycle.

TREND 8: CYBERSECURITY WILL DEFINE DIGITAL ECONOMY WINNERS AND LOSERS

The modern world is rapidly evolving into a digital knowledge-based 'industry 4.0' economy in a change as significant as the industrial revolution of the 18th Century. A fundamental challenge arising from this is how it should be secured, where the resources to do this will come from, and which global standards might be needed to smooth its development. The ability to resolve the challenge of securing the digital economy will define successful economies, business sectors, and perhaps even the political systems on which they are built. It is possible that for many large organizations this could come down to a simple scenario of success or failure with no easy middle way.



Trend 1: Cybersecurity has become a board-level issue

Until recently, cybersecurity was viewed as an IT challenge rather than a business risk. Despite years of warnings, it took until the aftermath of the NotPetya cyberattack in 2017¹ to change this view. Several large companies announced huge losses² caused by the incident, including shipping giant Maersk, FedEx, advertising company WPP, and home products company Reckitt Benckiser. All reportedly lost up to hundreds of millions each, making this the most expensive cyberattack in history. Meanwhile, data breaches continue to be a major cause for worry. Suddenly, cybersecurity has gone from being a hypothetical problem to an acknowledged business risk. This realization is now driving long-term changes in how cybersecurity risk should be managed, and by whom.



CYBERSECURITY HAS REACHED THE BOARDROOM

Cybersecurity risk has been added to a menu of problems which includes digital transformation and the early stages of the data and automation-driven economy of 'industry 4.0'. Self-evidently, cybersecurity is potentially a major barrier to the successful execution of these changes, which along with real-world losses and increased regulation has put it at the top of the to-do list for many boards. The way that cybersecurity is integrated into board decision making tells you a lot about the maturity of a business.

CYBERSECURITY HAS BECOME A COMPETITIVE ADVANTAGE

The stream of serious cyberattacks has turned cybersecurity into a disruptive force that is exerting tremendous pressure on even the most successful businesses. Organizations which handle this business risk at board level will find it easier to build secure and sustainable growth.

Similarly, enterprises that provoke an innovative cybersecurity culture will not only be secure, but also faster and more flexible than their competition. Successful organizations will be those able to cope with change positively and turn it into an advantage.

THE ROLE OF CISOS IS BECOMING CENTRAL

Enterprises with a mature and strong cybersecurity usually have a Chief Information Security Officer (CISO) who is a member of the board and reports to the risk-management department. The CISO is becoming essential for relating business objectives to increasingly complex cybersecurity risks that are impossible to predict. Identifying where these risks lie in any business strategy is something the boards shouldn't leave to chance, and that means being able to access expertise which can understand both technical and management perspectives.

CYBERSECURITY HAS BECOME A BOARD-LEVEL ISSUE



CYBERSECURITY IS VITAL FOR BUSINESS – CLIMATE OF ACCOUNTABILITY IS CHANGING



COST REMAINS A MAJOR BARRIER TO PROGRESS

Relating investment in cybersecurity to return on investment (ROI) is still not easy, even when expressed in terms of risk reduction. Organizations that achieve this are ones able to understand cybersecurity as innovation and not merely as an IT control that should be left to the IT department. Cybersecurity experts, meanwhile, must think about how to support continuous change and enable business growth by innovation. By aligning cybersecurity strategy with business strategy, the board has a chance to recognize that funding for fast, innovative and secure business growth is necessary.

AWARENESS OF MANAGEMENT ACCOUNTABILITY IS GROWING

While the idea that CEOs and management should be held personally accountable for cyberattacks is not a new phenomenon – think of the aftermath of the attacks on U.S.

retailer Target in 2013 and Sony a year later – it seems to have gathered pace in the aftermath of the attack on Equifax in 2017. This is a signal that the culture of accountability is changing and that even senior management are being asked to explain problems that might have happened several layers below their position. Increasingly, management must show that it provided the investment and decision-making structure to allow departmental specialists to handle data and mitigate risks, as well as designing adequate response systems in the event of a breach or attack. If we add the pressure of privacy regulations to this mix it becomes clear that cyberattacks are now helping to redefine how investors understand competent management.

1 The Untold Story of NotPetya, Wired Magazine, 9 September 2018

2 Manufacturers Remain Slow to Recognize Cybersecurity Risks, New York Times, 21 November 2018

EXPERT – WOLFGANG KIENER



WOLFGANG KIENER
Global Head, Advanced Threat Center
of Excellence, TÜV Rheinland

Wolfgang is responsible for the strategic service development in threat management globally. With more than 15 years of experience in major international corporations such as Siemens, T-Systems, Verizon and CSC, Wolfgang boasts extensive experience in the technical and commercial development of innovative cybersecurity services.

Trend 2:

Industrial cybersecurity is years behind mainstream IT security

An OT system is one where a computer controls or detects a physical action, which might be an electrical motor, a valve, or from a relay that has some sort of kinetic effect. For too long protecting these often safety-critical systems used by utilities such as energy, water and industry has been cybersecurity's poor relation, which has allowed complacency and under-investment to take hold. These days, new technology and geo-political tensions have fundamentally changed the risks of failing to protect OT, especially systems used to monitor safety. If something can be targeted, and at some point we must now assume it will be, we should do everything reasonable to avoid it being successful.

ATTACKS ON SAFETY-CRITICAL OT SYSTEMS HAVE BEGUN

The Triton malware attack¹ of 2017 was the first publicly-documented cyberattack on industrial control systems (ICS) that attempted to interfere with the workings of a Safety Instrumented System (SIS) used by an industrial facility to act as a failsafe against fire or explosion. As well as being a depressing milestone, this incident warned us that attackers are now targeting safety-critical systems and that the framework underpinning Triton will almost certainly become more widely available to others.

THESE ACT AS A PROOFS-OF-CONCEPT FOR NEW ATTACKS

With multiple threat actors researching similar attacks, it seems likely that the appearance and near success of Triton presages further serious incidents. While the vulnerabilities exploited in such attacks probably date back decades, what makes this type of threat potent is that these systems have in recent times been connected to the Internet for a host of operational reasons, the risks of which are only now being understood. A lot of this has been enabled through commo-

dity IT components and systems which introduce vulnerabilities of their own.

A SUCCESSFUL ATTACK ON OT OR ICS WILL HAVE POLITICAL CONSEQUENCES

Assuming a future attack is able to cause damage or disrupt an important economic asset, the pressure on private enterprises and governments for change will become overwhelming. In the past, such disruption was seen as either a theoretical worry or something for individual companies to take responsibility for. The flaw in this mindset is that the new wave of OT and ICS cyberattacks is by its nature about disrupting whole sectors, economies and political systems and this demands that regulators and politicians become more engaged or face a backlash.

REGULATIONS STILL LACK SUFFICIENT COMPULSION

The EU's Network and Information Systems (NIS) Directive requires states to identify and protect systems critical to their national infrastructure and to set up a Computer Security Incident Response Team (CSIRT) to aid defense in the event of an attack. However, a limitation with many similar

regulations is that they are largely advisory, telling organizations what they should do rather than what they must do.

EXPECT TOUGHER PENALTIES TO EMERGE AND SPUR INVESTMENT

One part of the solution is beginning to emerge. Increasingly, tougher penalties and jail time are making their way on to the regulation agenda. If companies managing safety critical systems don't invest in cybersecurity in ways that are later shown to have created vulnerabilities, then they will be hit with big fines and possibly even imprisonment for executives. Until this happens, there is a risk that managers will shrug their shoulders. In the field of health and safety legislation, the idea that a remote attacker could cause a major incident would not be tolerated and the same standard should apply to OT and ICS cybersecurity. In other cases, companies that lack the resources necessary to defend themselves because they are operating on tight margins, may need government incentives.

OT RISKS MUST BE BETTER UNDERSTOOD

Organizations in these sectors must urgently assess the risk in their OT and ICS, especially in safety-critical systems, by conducting a combined engineering and business review of organizational OT cybersecurity risks using an appropriate framework. Beyond that, they must develop a proportionate and measured remediation program, not forgetting the safety-critical aspects of some OT systems. This will also mean educating all parts of their workforce, including management and production staff as well as IT and security professionals. Finally, organizations must ensure that their supply chain meets their cybersecurity requirements, if need be by developing mechanisms to enforce this contractually.

¹ Nozomi Networks, Black Hat presentation Understanding Triton, the First SIS Cyberattack, August 2018

EXPERT – NIGEL STANLEY



NIGEL STANLEY
Global CTO, Industrial Security Center
of Excellence, TÜV Rheinland

Nigel is a specialist in cybersecurity and business risk with nearly 30 years' experience in the IT industry. He is a well-recognized thought leader and expert capable of delivering complex cybersecurity projects across small, medium and large-scale enterprises. He has written three books on database and development technologies and is a regular speaker at international events and conferences.

Trend 3: IoT cybersecurity faces a major standards challenge

Across the globe, standards bodies and industrial sectors are busily drafting the security and privacy standards necessary to secure the next wave of development in the IoT and OT. While the intention is good, this might result in a lot of confusion and wasted time as manufacturers attempt to work out which of these regional and sector-specific efforts they should comply with. Particularly at risk are global businesses that depend on having an understandable path to compliance to smooth their product development. As competing standards vie for importance, time could be wasted.



THE DEVELOPMENT OF IOT STANDARDS IS INHERENTLY COMPLEX

The solution to weak IoT security should be to develop standards which can be adopted by all manufacturers at an architectural level. Unfortunately, while this is a good approach for consumer devices which are very similar to one another, it can prove limiting for industrial and OT applications where the ability to customize equipment for diverse applications is essential. The risk is that security and design flexibility end up at odds with one another, slowing down deployment. Ultimately, standards will need to be tailored for each area of industrial IoT, for example the automotive sector as compared to ICS. Inevitably, this is going to take time which means progress will be measured in years.

REGULATION IS BEST DRIVEN BY INDUSTRY

Worries over the state of IoT and OT security have reached government level, creating pressure for greater regulatory attention. The danger is that there is a drift towards regional standards that seek to impose compliance to U.S., E.U. or Asian regulations. This approach could be a short-term fix which in the long run could result in higher costs and greater confusion as organizations find it difficult to understand the risks associated with the expansion of interconnected devices. Another danger is that regulation creates a means to block or restrict the global trade of these devices which are important for healthy innovation. Under that scenario, standards could become a barrier rather than an enabler.

IOT SECURITY IS BECOMING A SAFETY ISSUE

Incidents of weak IoT security have become a common occurrence with the best-known examples primarily involving consumer devices that compromise data and privacy. The emergence of more sophisticated examples such as the VPNFilter router malware¹ underline how this trend could get worse before it gets better. Nevertheless, there is a growing recognition that in the industrial context, this could be serious enough to compromise the safety of physical devices in ways that are dangerous to people. All that is needed to tip this from a theoretical issue to a real one is the motivation to do it, which could be anything from business competition and cyber-extortion to geo-political rivalry.

GLOBAL STANDARDS AND INDUSTRY BODIES NEED INVESTMENT

Government involvement in industrial IoT security is unlikely to gain traction quickly enough and would be better directed towards the regulation of breaches and security incidents in ways that incentivize IoT makers to take security seriously. It would be far better to encourage a greater role for global standards bodies such as the International Electrotechnical Commission (IEC) which has a proven track record for smoothing the path of previous waves of innovation such as electrical generation and transmission. It's not yet clear whether there is enough consensus to adopt this currently, which leaves the industry to fall back on the continued development of best practices of the sort emerging from private organizations such as the Open Web Application Security Project (OWASP).

¹ New Router Malware with Destructive Capabilities, Symantec, May 2018

EXPERT – NATHANIEL COLE



NATHANIEL COLE
Global Head, Cybersecurity Testing Center
of Excellence, TÜV Rheinland

With more than 15 years' experience, Nathaniel provides recommendations for the remediation of vulnerabilities and insecure systems. He is an advocate on how security should be implemented in different industries, including manufacturing automation, IoT and robotics. He is an expert on testing devices, including robotic systems, and medical and wireless devices, to show how security impacts their usability, integrity, and safety.

Trend 4:

The pressure created by GDPR represents a turning point for consumer privacy

Within months of the European General Data Protection Regulation (GDPR) coming into force in May 2018, the first trickle of prosecutions became public, including € 50,000,000 fine imposed by the French data protection authority CNIL on a major search engine operator for not „clearly and comprehensibly“ informing its users about the use of their personal data.

Although this represents a slow start and the early fines have been modest in size, it is becoming clear that the GDPR will be a major influence on privacy across the whole world and not only in the E.U. itself. For most industries, it will simply be cheaper to design their products and services to conform to the highest global standards rather than geographically-defined privacy.

IOT WILL BE AN IMPORTANT TEST BED FOR THE GDPR'S EFFECTIVENESS

The implications of this are starting to be realized in sectors such as the IoT, which has often been taken up by industrial companies with little or no expertise in traditional IT security. One effect of GDPR in this sector will be to increase the costs of developing devices in ways that will be passed on to consumers who have grown used to buying products based primarily on their price. This sets up a conflict between the need for greater privacy and security and the difficulty of persuading consumers to pay for it. This is especially true for the growing number of devices already on sale and which might need to retrofit better privacy and security controls in ways that developers could struggle to fund.

REGULATION ALONE IS NOT ENOUGH

Currently, there is a surge in new IoT devices that will remain active for a decade or more into the future, including smart energy meters, smart televisions, home security, IoT-aware broadband routers, smart speakers, and in IoT connectivity for connected cars. This tends to be understood as a technological enablement of previously 'dumb' devices when in truth it is really a trend to turn such devices into information-collection sensors. A major problem with this is that it makes the privacy implications largely invisible to consumers who can't see how information is being collected, nor the risks it creates. Consequently, simply regulating for better privacy on these devices will not be enough on its own, while understanding of the principles of privacy among consumers remain weak

GDPR – AN IMPORTANT MOMENT FOR PRIVACY WORLDWIDE



FIRST IMPACTS OF GDPR SINCE MAY 2018



First big fines
for infringements
50,000,000 €



Increasing costs for manufacturers
of IoT devices because of severe
regulations and invest in R & D
and product development

Improved security
for IoT devices
because of



Severe
regulations



Increasing customer
awareness



Certifications:
GDPR recognize
certification
bodies

NEXT BIG CHALLENGES



Certifications



Higher privacy
standards



Higher demand
for products and
services compliant
to GDPR

globally. Consumer feedback represents an important business pressure that is still not being felt.

PRIVACY NEEDS MORE INVESTMENT

IoT in the E.U. and beyond needs clear regulation and effective accreditation - someone must be on hand to check what devices are doing and how their design might affect privacy. Ideally, this will lead to a situation where every device or service clearly explains what it is doing, not

simply in terms of its technical functions but its information collection and processing. From industry, this demands investment from R&D, product development and even marketing. Companies must think about how privacy affects the products they sell throughout their lifecycle and build this into their business models. Conversely, regulators must invest in the resources needed to hold the private sector accountable through testing, accreditation and compliance.

EXPERT – UDO SCALLA

Having worked in executive positions in the CE and ICT Industry (Deutsche Telekom/T-Systems/Technisat) Udo's focus is now on IoT cybersecurity, privacy/ethics, and the implications of EU's GDPR. In 2015 he co-founded CorDev GmbH, which in 2016 received the award for the best German start-up for the smart home industry from the Federal Ministry of Economics.

UDO SCALLA
Global Head, IoT Privacy Center
of Excellence, TÜV Rheinland



Trend 5:

The cybersecurity skills shortage will distort the labor market

The surge in the importance of cybersecurity has come at a time when the skills required to strengthen it are in critically short supply. By 2020, globally this could reach 1.5 million, with some estimates putting the figure at more than double this by 2021. Under such an extreme skills shortage, market distortions start to occur, with larger, wealthier organizations and service providers able to attract talent while smaller companies in some sectors struggle. Inevitably, this not only makes cybersecurity more expensive but impacts supply chains that tie the economy of large and smaller companies together. For the long-term interests of the emerging industrial economy, cybersecurity is a common good that should be accessible to all. Failure to address this problem is to store up problems for the future.



THE CYBER-SKILLS SHORTAGE IS WORSENING AT A BAD MOMENT

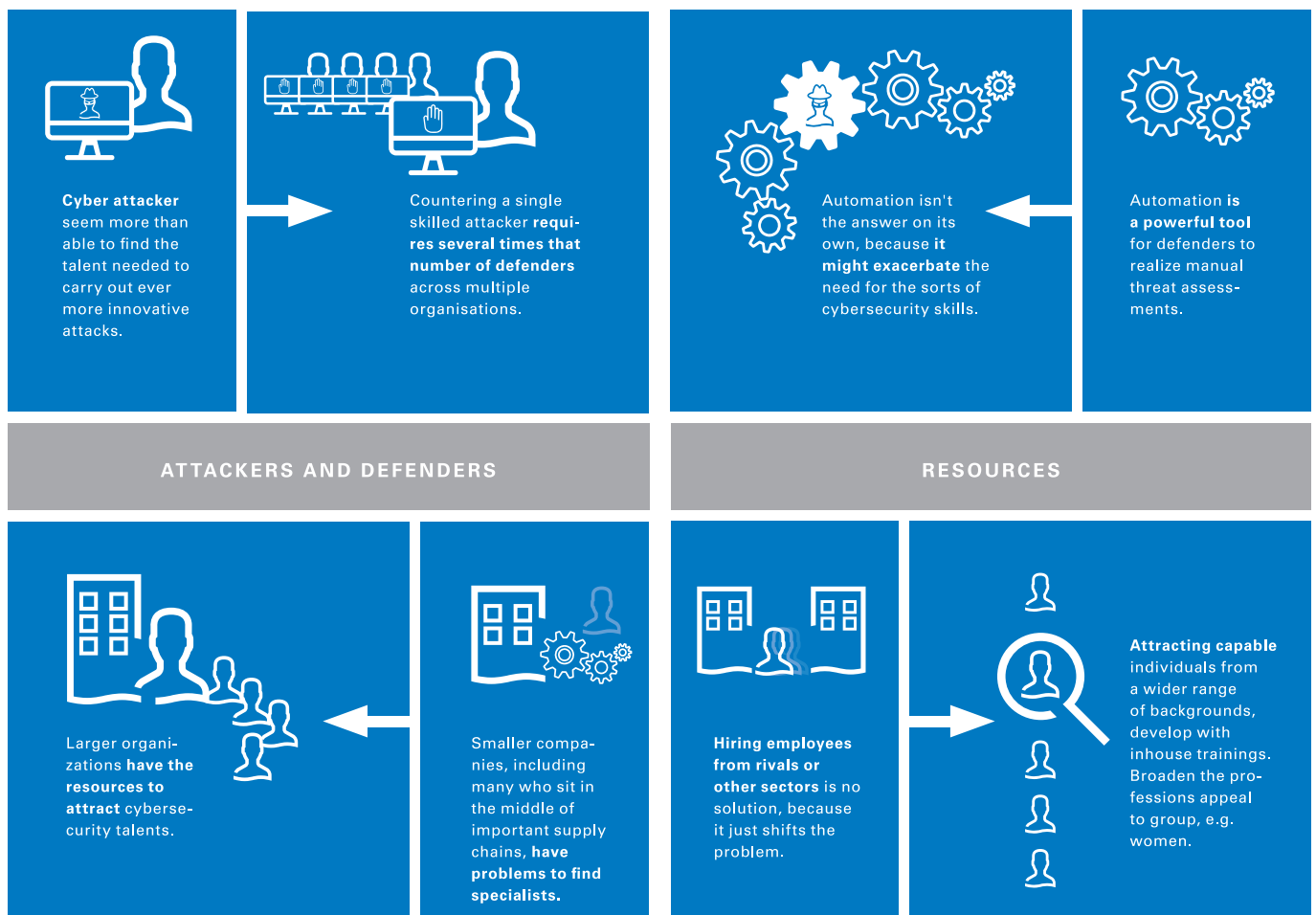
The rapid evolution of the IoT, the digitalization of the economy, and growth in industrial automation is increasing the number of devices attackers can target and outstripping the skilled employees required to defend them. Ironically, the same calculation doesn't apply to cybercriminals, who seem more than able to find the talent needed to carry out ever more innovative attacks. It's a skills asymmetry that helps cybercrime to flourish – countering a single skilled attacker requires several times that number of defenders across multiple organizations. Unfortunately, the attackers understand their advantage and are gaining confidence that the balance of power is tilting in their direction.

A LACK OF SKILLS LEAVES SMES EXPOSED

While larger organizations have the resources to find cybersecurity talent, the same is not true for smaller companies, including many who sit in the middle of important supply chains. This presents a challenge for entire sectors – larger organizations can defend themselves but not the numerous smaller organizations they depend on, some of which might be in countries beyond the reach of the regulations that apply locally. One solution is for SMEs to tap into the managed security service provider (MSSP) sector but many of these are enterprise-focused and don't necessarily understand the problems faced by small businesses.

THE CYBERSECURITY SKILLS SHORTAGE REQUIRES NEW THINKING

Challenge of the asymmetry ... that helps cybercrime to flourish.



INDUSTRY 4.0 WILL RELY HEAVILY ON CYBER-SECURITY

Industry transformation over the next decade will depend on finding the expertise to marry production knowhow with cybersecurity concepts that have their origins in IT. One challenge is that industrial cybersecurity in production environments and IT skills remain distinct areas of expertise, which makes it even more difficult to find people who understand both. Attackers will, inevitably, seek to target production systems if this very specific skills shortage is not addressed.

AUTOMATION ISN'T AN ANSWER ON ITS OWN

One possibility for bridging the skills shortage is to automate manual threat assessment, using human intervention only where necessary. While automation is a powerful tool for defenders, it is also possible that it might exacerbate the need for cybersecurity skills, particularly in areas such as artificial intelligence, machine learning, forensics, and response. At best, automation might simply allow organizations to keep up with the pace of cybercriminal innovation while requiring them to hire engineers with new skills that prove hard to find.

THE CYBERSECURITY TALENT POOL MUST BE EXPANDED

While universities and apprenticeships offer a possible solution in some countries, a longer-term approach would be for larger organizations to stop simply hiring employees from rivals or other sectors and instead consider investing in programs to develop them inhouse. It could also prove fruitful to look beyond candidates with specific formal qualifications or types of experience as a way of attracting talent from a wider range of backgrounds. One example of this would be to broaden the profession's appeal to groups - women being the obvious example - which cybersecurity has traditionally struggled to attract. The old approaches to recruitment need to evolve – the size of the recruitment gap is a constant reminder of the need for change.

EXPERT – BJÖRN HAAN



BJÖRN HAAN
Managing Director of Cybersecurity,
TÜV Rheinland

Björn has 23 years of professional experience in large international enterprises, which has had a lasting impact on his entrepreneurial skills. He started his career in 1994 at Ploenzke AG as a management consultant, before moving to IBM in 1999. There he was responsible as manager for various national and international areas connected to IT strategy and costs, business value and, more recently, spent more than five years with IBM's Cyber Security business in Western Europe. Since 2011, he has been responsible for the businessfield Cybersecurity in Germany at TÜV Rheinland.

Trend 6: Threat detection and response depends on maturing Security Orchestration, Automation, and Response (SOAR)

Security Orchestration, Automation, and Response (SOAR) has huge potential to reduce the time to detect and respond to incidents and minimize the impact of cyberattacks. The biggest benefit may be automated containment workflows, which are critical when dealing with fast-spreading destructive malware. Other benefits include standardizing investigation processes, accelerating prioritization and response, enabling proactive threat hunting, and improving the quality and efficiency of detection and response processes. However, implementing a new wave of automation requires investment and planning from organizations during a period when established investments such as Security Information and Event Management (SIEM) are still bedding in.



AUTOMATION IS BEING DRIVEN BY EVOLVING CYBERATTACKS

The last year has seen a continuing roll call of cyber-incidents, including large data breaches, the probing of critical systems and even the ransoming of municipal infrastructure. The root causes include past under-investment, expanding attack surfaces (IoT, the cloud, mobile, and social media), as well as advances in the tools and techniques used by attackers. Attackers continue to evolve new techniques as the tools to aid their incursions become commoditized. Unfortunately, too many organizations lack the capability to detect and respond to attacks quickly enough to significantly reduce business impact.

TRADITIONAL EVENT MANAGEMENT SECURITY IS UNDER PRESSURE

SIEM is now evolving into big data analytics with machine learning. This evolution is happening at different paces among vendors. In the meantime, we see various approaches from organizations staying the course, complimenting traditional SIEM, and even replacing or foregoing it in favor of modern big data analytics solutions for behavior-based threat detection. To take advantage of SOAR an organization must have a reasonably mature security program. Automation and orchestration capabilities are being added as features of many security products, particularly SIEM and endpoint solutions. Organizations may focus on more limited capabilities within a single product before investing in holistic solutions.

NEW TECHNOLOGIES NEED TIME TO MATURE

SOAR is still a relatively young and emerging technology designed to integrate existing and future technologies through well-defined processes. Therefore, out-of-the-box turnkey solutions will rarely work. Success hinges on bringing in the right data to make informed decisions, executing strong formalized processes based on those decisions, and integrating the right technologies. These components will vary greatly among organizations and require significant

expertise to build, test, and manage successful SOAR solutions. The path to success is for organizations to have the right foundational security technologies in place to make informed decisions as they automate processes.

ATTACKERS CAN DEPLOY MALICIOUS AUTOMATION OF THEIR OWN

Attackers have been leveraging and increasing automation for a long time and the pace of this evolution is quickening. Recently, we've seen evolution in malware's scripted capabilities to identify and exploit vulnerabilities and then move through a range of post-exploitation activities (privilege escalation, lateral movement, defense evasion), often employing multiple tactics and techniques very rapidly. We should expect to see continued automation across the full attack lifecycle and the integration of machine learning in the future.

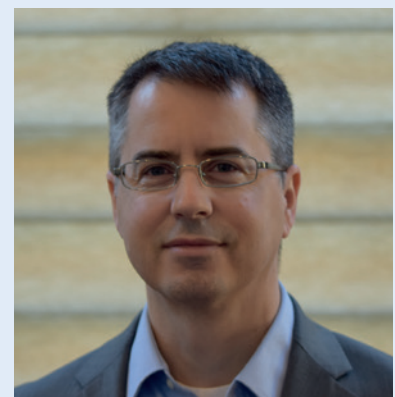
HUMAN INTERVENTION REMAINS AN ESSENTIAL INGREDIENT OF CYBER-DEFENSE

The rise of automation isn't a magic fix for deeper problems such as the skills shortage, indeed it might even create more demand in the short term as these technologies develop and are deployed. The key decision-making in Security Operations Centers (SOCs) must still be made by humans for a range of operational, regulatory, and legal reasons. What automation brings is the ability to make these decisions more rapidly than in the past, based on more data, and with greater certainty. However, allowing a wider range of organizations to access this sort of expertise will require the development of affordable managed services providers, which will thrive in the new world. The good news is that while threats and risks increase, the industry is continuing to innovate with cybersecurity solutions. TÜV Rheinland sees more organizations that are making significant investments to protect themselves and their customers and have measured success in detecting and rapidly containing advanced threats.

EXPERT – BRIAN NOLAN

Brian is a cybersecurity executive leader with over 20 years of experience in information security and risk management. For the past 14 years Brian has held progressive leadership roles in management consulting and technical services with extensive involvement in helping large organizations across diverse industries evaluate, build and enhance all aspects of their information security programs.

BRIAN NOLAN
Global CTO, Advanced Threat Center
of Excellence, TÜV Rheinland



Trend 7: 'Red team' testing and agile security development are gaining greater mainstream acceptance

From its origins in the penetration-testing sector, red team or 'holistic' testing is the trend to simulate how an attacker might penetrate an organization under real-world conditions by exploiting any available weakness to gain access to a resource. While flaws can be found in many resources – applications, devices or infrastructure – red teams also look at broader issues such as social engineering, hijacking a social media presence, physical access to a building or, in the most challenging cases, malicious insiders. Unlike traditional pen-testing, red teaming tries to understand how these operate together rather than as a series of separate layers. Working in tandem with this is the rise of agile security testing, which aims to remove as many software vulnerabilities as possible during the development cycle.



THE BENEFITS OF RED TEAM SECURITY ARE NOT ALWAYS APPRECIATED

The ultimate purpose of a red team attack is to improve the performance of defenders, the blue team, in a feedback loop of improvements. Despite this potential benefit, awareness of red team testing remains low outside the U.S., including in Europe which is perhaps two or three years behind in terms of mainstream acceptance. In these geographies, red team testing is still seen as a specialized form of pen-testing rather than something many larger organizations looking for higher risk maturity should consider. Interest in the benefits of red team testing are likely to grow but this could still take several years.

CYBERSECURITY DEFENCES REMAIN FRAGMENTED

A major weakness is that IT departments have traditionally focused on a form of defense that breaks down the security into individual problems that are the responsibility of specialized engineers. Too often, there is no single individual whose job it is to take responsibility for all aspects of security, including physical security and staff behavior. This is a structural problem that puts defenders at a disadvantage because there is a built-in tendency to fix problems piecemeal rather than understanding how weaknesses overlap and interact with one another. Attackers, meanwhile, are unburdened by these constraints, understanding targets as offering many simultaneous avenues for compromise.

FINDING THE RESOURCES TO IMPLEMENT RED TEAM TESTING CAN BE A PROBLEM

Despite growing interest in red team testing, funding this kind of undertaking is still the sort of demand that even well-resourced organizations can find hard to justify in terms of a traditional cost-benefit analysis. In some cases, IT departments might see it as either undermining their role, or as secondary to the primary job of minimizing risks

using conventional cybersecurity defences. There is also some confusion about the difference between red team testing and a conventional penetration test of the sort many organizations already carry out periodically.

AGILE SECURITY DEVELOPMENT IS COMING OF AGE

The traditional 'waterfall' notion that security testing is an optional bolt-on is giving way in many sectors to a new understanding that software teams need to integrate security testing as part of the development cycle. The calculation is simple - removing flaws at this stage is both easier and cheaper as well as more secure in the long term. In an agile development process, this demands continuous code testing using both automated and manual processes. The importance of this trend is that security testing is not only adding to development cycles but changing them too. A limitation remains that security testing is not always well understood. During 2019, agile security testing presents internal and external development teams with cultural as well as technological challenges.

GDPR WILL BECOME A POSITIVE INFLUENCE

The arrival of the GDPR and the possibility of large and very public fines is encouraging the management of high-risk organizations to rethink how they assess their security and response on an organizational rather than departmental or application-specific level. Specifically, Article 32 (section 1) states that organizations should have *"a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing."* Red team testing, commissioned at board level, offers one route to achieving this that can overcome organizational resistance or special interests. Unlike a conventional penetration test, a red team test offers an opportunity to crystalize risks in a way that can help to guide future investment.

EXPERT – DANIEL HAMBURG

Daniel holds a PhD in electrical engineering and has more than 10 years of professional experience in information security. For the last 8 years he has been responsible for Testing services at TÜV Rheinland. His team performs technical security analysis of applications, infrastructures, embedded systems, including IoT devices and automotive components. In addition, Daniel is a professor for IT security at the University of Applied sciences and Arts in Dortmund.

DANIEL HAMBURG
Regional Segment Manager, Cybersecurity Testing,
TÜV Rheinland



Trend 8: Cybersecurity will define digital economy winners and losers

The modern world is rapidly evolving into a digital knowledge-based 'industry 4.0' economy in a change as significant as the industrial revolution of the 18th Century. A fundamental challenge arising from this is how it should be secured, where the resources to do this will come from, and which global standards might be needed to smooth its development. The ability to resolve the challenge of securing the digital economy will define successful economies, business sectors, and perhaps even the political systems on which they are built. It is possible that for many large organizations this could come down to a simple scenario of success or failure with no easy middle way.



REGULATION, STANDARDS AND NORMS STILL LAG THE CYBERSECURITY PROBLEM

Despite developments such as the GDPR, the standards necessary to regulate security and privacy remain weak, often outpaced both by new technological possibilities and the risks created by cybercrime itself. There is similar work to be done on accreditation, the processes for which are emerging only slowly in the E.U. The ultimate expression of this is the way that geo-political rivalries have fueled a dramatic growth in attacks blamed on nation states. Without the norms, treaties and communication channels that have existed in the physical world, such conflict risks creating a highly unpredictable march towards escalation. Simply getting nations to agree on a common set of principles governing free market and national behavior in terms of privacy and cybersecurity presents a huge political challenge.

CYBERSECURITY IS BECOMING A BRANCH OF BIG DATA ANALYTICS

Given the dramatic rise in data volumes, the use of big data analytics is arguably the only way organizations will be able to cope with the expanding security problem – simply tweaking SIEM rules on its own will not be enough. A key element of this is statistical anomaly detection and response based on defining what is ‘normal’ inside an organization at any moment in time, the so-called zero-trust security model. That said, not all organizations can afford to invest in these technologies or have the expertise necessary to implement them, which implies that the development of a mature services sector will be key.

AUTOMATION AND MACHINE LEARNING CUT BOTH WAYS

Cyber-defense is becoming less about whether an organization can stop attacks but how quickly and competently it can respond to them once they’ve happened. This is driving

the growing trend of cybersecurity automation and machine intelligence because it is only through such processes that organizations have any hope of coping with this reality. At the same time, there is a growing worry that cybercriminals might start using the same automation technologies to increase the effectiveness of their attacks, which implies a machine learning arm’s race. It seems likely that the first attacks utilizing early elements of this will be detected during 2019 which will spur further investment.

CYBERSECURITY HAS GONE FROM IT PROBLEM TO STRATEGIC WEAKNESS

Today we are seeing a dramatic expansion of digital capabilities, data and devices as organizations look for a path to define what a digital version of themselves might look like. However, this has created a larger surface for attackers to aim at – it’s as if organizations are trapped between the need to fully digitalize their business models but without the cybersecurity standards and access to the trained workforce necessary to achieve this without increasing risk. The solution should be an expansion in the skills base, but this is easier said than done given that the gap between the number of open positions and suitable applicants is widening. Automation and machine learning offer a potential escape but these, too, require, skills that are hard to find. This underlines how cybersecurity is fast becoming a weakness that could separate winners from losers and an economy in which only the brands with the deepest pockets will survive. It’s the sting in the tail for business which until now have seen online technology as a way of finding new markets and enabling new possibilities. While that remains as true as it’s ever been, the risks it has created are potentially existential.

EXPERT – ANTHONY DICKINSON

Anthony heads TÜV Rheinland’s Centres of Excellence for Digital Transformation and Cybersecurity business, where he leads the creation, execution, and evolution of its business strategy. He has spent over 20 years in technology, working for both global brands and smaller boutique firms advising senior executives on business technology and product strategy. A strong believer that there’s nothing more practical than a good theory, he takes inspiration from diverse domains including, strategy, complexity, evolution, psychology, neuroscience, leadership, and productivity.

ANTHONY DICKINSON
Global Head of Strategy,
Digital Transformation & Cybersecurity,
TÜV Rheinland



TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Cologne, Germany
cybersecurity@tuv.com

www.tuv.com

