NTT Security 2018 Security Trends & Predictions

What will shape the next 12 months in cybersecurity?

DevSecOps in the age of the cloud

DevOps is an increasingly popular development practise allowing organizations to increase the speed at which they produce apps and services. An unfortunate side effect of this process is that you might also be accelerating the production of insecure code and bugs, with the potential to cause a serious financial and reputational hit if not managed correctly.

In an increasingly cloud- and mobile-first world, it will become essential to also bake in security to this process: thus, DevOps becomes DevSecOps. Embracing an application lifecycle approach in this way will end up saving organizations time and money – because problems are always easier to solve when security is addressed as far 'left' in the lifecycle as possible. It will not be an easy shift for many security professionals, but third-party expertise will help overcome cultural resistance and arm organizations with the right processes and automated toolsets to drive success.

Machine learning and managed security

Machine learning, AI and automation have the potential to plug chronic security skills shortages and transform threat defence by spotting sophisticated advanced attacks and zero-day threats. Whatever the industry marketing hype might have you believe, machine learning is actually far from new – in fact, NTT Security has been using it for 15 years.

Machine learning is not a silver bullet and should instead be used as part of a layered approach to threat prevention. But it can spot patterns, which human eyes might miss. That said, it shouldn't be seen as a replacement for human expertise. Part of the value we offer is in arming Security Operations Centre experts with machine learning tools. The automated tools find the needle in the haystack, but then it's vital to get human eyes on that needle to analyze it further.

These kinds of capabilities are set to drive a surge in managed security services (MSS) next year and beyond. In fact, according to our Risk:Value 2017 report, 44 percent of organizations globally are using or planning to use an MSSP, with 28 percent claiming this is because of the lack of internal skills and 29 percent because they want access to better tech. Just be sure to conduct thorough due diligence before choosing a third party.

From tech- to business-driven security

Security professionals love to talk bits and bytes, sometimes even 'out-geeking' the rest of the IT department. But we are already seeing a change taking place, and it is a necessary change: in fact, it's a question of digital survival. Put simply, security strategy must be aligned to business strategy or vital digital transformation projects will fail and the business will become irrelevant. Some 85 percent of business leaders believe they only have two years to make progress in their digital transformation programs before they fall behind their competitors.

Honourable GDPR mention

2018 will be the year when the GDPR (25 May) and NIS Directive (9 May) come into force. I won't add to the thousands of opinions already circulating about this but, suffice to say, it's vital to get your compliance house in order asap. If organizations are having trouble getting the board's attention, remind them of the maximum fines for non-compliance: £17m or 4 percent of global annual turnover, whichever is higher.

Log collection and analysis

Organizations will increase the amount of log data they collect and need to analyze. They'll look to high-speed platforms to help with searching and analyze the large amount of information they will collect. This will help with detection and threat hunting activities. Part of that analysis may include machine learning and assistance with pattern recognition and behavior anomalies. While mature organizations will be more selective of the data they collect based on their detection requirements, overall the volume of data will continue to increase. Along with this increase in overall volume, there is a need to search and analyze this data as quickly as possible.

Cloud usage

Organizations will continue to leverage cloud services. While some organizations are just moving to cloud computing (IaaS), other are fully adopting the cloud and using Software as a Service (SaaS). While a certain level of security comes along with some of these cloud vendors, clients will ultimately still be responsible for the protection of their data, no matter what environment that data exists in. Cloud Access Service Brokers (CASB) and other cloud auditing capabilities will become more predominant in the marketspace and a necessity for organizations.

IoT

Especially at home, the number of IoT devices will continue to increase. On the commercial side, Operational Technologies (OT) will gain more traction in automated factories and critical infrastructure. The protection of these is important from many different avenues including protection of human life and usage in large scale cyber attacks. As more of these devices are deployed and used, the security with them continues to be highly immature and organizations do not properly deploy and protect these technologies.

Organizations will seek a new formula to calculate risk

Recent high-profile breaches suggest that some organizations may still be taking a gamble when it comes to cybersecurity maturity. Our recent Risk:Value report estimates it takes upwards of $1million to recover from a breach – though that does not take into account less tangible costs such as customer trust and brand reputation. As examples of high profile breaches continue, and the costs of an impact escalate, organizations will need to consider new metrics to calculate acceptable risk. This may not mean they change their risk profile immediately, but it will, at least, mean they are more aware of their exposure to breaches and their likely financial impact.

Mistakes will still happen

Not all the high-profile breaches in 2017 were due to cybercrime in the first instance. Many are still as a result of poor data handling. This is likely to continue until organizations implement processes and procedures for good data management across the whole of the organization, and measure their employees against them. 2018 could see a greater emphasis on incident response planning and processes, and potentially see cybersecurity linked more widely to overall HR policies and employee objectives in an effort to install a culture of awareness and responsibility throughout the organization.

Cybersecurity to play a greater role in digital projects

It has been described by some as the next industrial revolution and one thing is for sure, the rapid pace of the digital era is leading to digital disruption and a huge rise in digital transformation projects. In the excitement of using new technologies for competitive advantage, or indeed the fear of being left behind by digital applications, it is perhaps easy to see how cybersecurity could get overlooked in the race to take first mover advantage. As recent high-profile examples illustrate, this could be a costly mistake. To truly maximize the opportunities that digital transformation provides, 2018 may see cybersecurity playing a crucial role in unlocking the true value of these projects. If consumers have confidence that the new digital applications they use offer both benefits and security, they are more likely to adopt them – and continue to use them.

The end of 'passive trust'

2017 has seen huge breaches of customer data, ranging from names, contact details and financial information. Understandably, this has been met with anger from customers who trusted those organizations with their personal information. There is a recognition that personal data has value – not just to the organization it is provided too, but also for the purposes of cybercrime. GDPR will of course help sharpen the focus of organizations in regards to the management of personal information, though 2018 is likely to see a wearier consumer who will be less likely to freely share their personal data or, perhaps, provide minimal or less accurate information in the first place.

Quality assurance will need assured quality

Quality assurance is an essential part of consumer trust and is especially important for mission critical applications and precision products. With the increase of operational technology (OT) and quality control systems becoming digitized, the risk for compromise from cyber criminals heightens. If the quality process is compromised, the consequences could be catastrophic. 2018 is likely to see the adoption of security controls to protect vulnerable but critical systems as they become increasingly revolutionized by new, disruptive technologies that drive efficiency gains for organizations.

Critical Information Infrastructure (CII) demands

We will see increasing demands on Critical Information Infrastructure (CII) to improve their cybersecurity. CII typically refers to sectors that are responsible for the continuous delivery of essential services in a country, including government, information communications, energy, aviation, maritime, transport, healthcare, banking and finance, water, security and emergency services, and media. On any given day, the chances are that if you work in a CII sector, you have had to fend off cyber attacks. Activist groups, individual troublemakers, criminal organizations and rogue states are targeting both Information Technology (IT) and Operational Technology (OT) and our CII daily, in an attempt to disrupt services and cause havoc.

In June 2017, the Petya ransomware attack hit airlines, hospitals, banks and utilities around the world, causing them to shut down their computer systems. Three months earlier, the global WannaCry ransomware attack closed parts of the UK's National Health Service causing it to run some services on an emergency only basis. In October 2016, the Mirai malware created botnets on IoT devices to launch a massive distributed denial-of-service attack that disrupted all US internet traffic.

The last thing that any organization wants is to make the headlines following a security breach. The damage to reputation can be enormous, as can the financial costs. The first step in controlling risk is to understand your exposure across all areas of the business and prioritize those deemed critical. It's not a case of if it will happen, but when it will happen, so it is essential that you have a mature, detailed incident response plan, and monitoring systems capable of providing a comprehensive and real-time view of network activity. Timely incident response is imperative following a breach and many organizations don't have spare resources waiting to leap into action when an incident happens. It might be worth considering a monitoring and incident response partner to provide the right resources to help you return to business as usual as quickly as possible should a breach occur.

GDPR will force organizations to assess their wider data security practices

With GDPR fast approaching, organizations are realizing they have no easy way to map all of their critical data, whether unstructured, structured, or big data, and monitor how it is processed or controlled in a complex infrastructure of virtualized, on-premise and cloud environments. With the principles behind GDPR focused on securing data and privacy 'by design', security teams will be looking to implement a strategic approach for integrating security tools into the data lifecycle, to avoid hefty fines and ensure they keep a competitive edge as a trusted organization.

Attention will be turned inside-out

Insider threats are becoming a greater risk to businesses, not just in terms of negligent or malicious employees, but also in terms of the collaboration from external attackers. Attackers are increasingly using techniques such as advanced phishing and social engineering to steal privileged credentials, which allows them to move inside sensitive networks by masking themselves as trusted employees. Security teams will need to start looking at using the right combination of technology, people and processes to put in place a robust insider threat program and this is where we can potentially see Managed Detection and Response (MDR) services playing a bigger role in the industry.

Organizations will require cloud-delivered security to fit their cloud plans

2018 will see an increased adoption in cloud-based security services, in order to have quicker access to advanced enterprise security that can scale at the pace of digital transformation. As cloud projects are implemented in order to keep operational costs down and streamline efficiency, the same requirement will be expected of security. However, managing multiple technologies in hybrid environments will require working with a strategic Managed Security Services Provider (MSSP) in order to provide a central interface for monitoring these assets and funnel the huge number of alerts into critical incidents, as opposed to being bombarded with false positives.

Skills shortages will be critical factor in enabling digital transformation

Organizations will continue to transform their digital assets in order to optimize their time-to-market and customer experiences, however 2017 has shown us that not embedding cyber resilience into these projects can mean losing customers and spending huge amounts to recover from breaches. This has been partly due to poor security practises, but also due to the lack of security skills to cope with new technologies, both in IT and security. Organizations will need to assess whether they have the right skills in place to enable digital transformation whilst responding to the inevitable onslaught of advanced cyber attacks.

Incident response will require better incident readiness

The constant rounds of large scale breaches in 2017 has given organizations a lot to think about, especially how best to respond to an attack. Our 2017 Risk:Value report showed that organizations expect to take an average of 74 days to recover from a breach. Proactive measures will be looked at in order to better prepare for Advanced Persistent Threats (APTs) and ensure business disruption is kept to a minimum. This will require a robust and flexible partnership with security experts who can implement the right processes and controls from the start but also respond quickly to an attack, should the worst happen.

Digital transformation projects require a different cybersecurity approach

Digital disruption is all around us and, for organizations to be agile and dynamic, they need to build in cyber resilience into the business. We've seen numerous headlines regarding breaches and the cyber threat and we have, for many years, stated that security shouldn't be an afterthought. Cyber resilience has to be designed into the business processes so you can take advantage of digital transformation and the business opportunities this provides.

Securing the cloud is so tomorrow

Businesses have to determine now, where the cloud is and how the individual is leveraging this to meet business demands. So securing the workspace of the worker of tomorrow is paramount and leveraging smart working practices is essential. IoT is pushing the cloud to the edge and closer to the processes and devices that make up our business environment. These need to be secured and leveraged to provide optimized business, to proactively manage the individual and machine alike.

Customer intelligence without breaking data privacy

The focus on customer satisfaction and intelligence requires a very different information security model – one that analyzes data without undermining privacy. Encryption models and obfuscation require a completely new approach particularly with regards to quantum computing. Or we have to accept that to be secure we have to give away some of our privacy.

Digital business has to focus on integrity and availability

Availability is essential to the digital business but so is integrity. As our world becomes paperless and online, it is essential that integrity of data is embedded into the systems and processes not only with regards to cash, but with everything about the individual. Our physical footprint is diminishing and even then our physical devices interact digitally. Integrity and verification will be paramount for trust to be established in a digital world.

Devices, devices everywhere but not a secure one in sight

Clearly IoT is getting a lot of press at the moment and we can clearly see the business benefit of collating and analyzing our business systems and devices along with the employees and customers that use them. But as we have seen too often in the past, security is an afterthought. Businesses will start to see the benefits of collating data that allows proactive remediation before the business is impacted. However, understanding and securing the massive amounts of data will require a different analytics approach. Cybersecurity might not be the first thought when analyzing a sensor on a production line, but we have to get used to the fact that, if we can see the data and modify the controls, then someone else can too.

Contributions from our NTT Security experts including:

Kai Grunwitz, Senior Vice President EMEA; Bryan Pluta, Director, Enterprise Security Services; Stuart Reed, Senior Director; Richie Tan, Head of Security Consulting, APAC; Ben Chant, Market Insights Manager; and Garry Sidaway, SVP Security Strategy & Alliances.

To learn more about NTT Security and our unique services for information security and risk management, please speak to your account representative or visit: **www.nttsecurity.com** for regional contact information.