What I wish I'd known

Future of cyber

To counter new and morphing threats, leaders in cyber security will count on cyber hygiene, automation, security by design, counterintelligence, recoverability and regulation.

175zb

predicted collective sum of the world's data by 2025

Seagate 2018

Known knowns

The future of cyber security is closely intertwined with the future of technology and the IT systems that must be protected. It is therefore instructive to start with a brief overview of key technology trends that are relevant for cyber security.

Since its inception, the performance of IT has grown exponentially and we can expect that the speed and capability of our computers continue to increase every couple of years, as outlined in Moore's Law[1]. Technology adoption is also growing exponentially, as seen by the speed at which mobile phones, drones, cloud computing and even games like Pokémon Go have achieved omnipresence[2]. Digital has spilled over into our social, psychological, and political lives where clever IT systems shape our opinions, beliefs, biases and preferences.[3]

This has also led to an exponentially attack surface – the number of touchpoints of IT systems

that allow attackers to reach and exploit them. The bigger the attack surface, the harder a system becomes to secure and the easier it can be hacked. This is most evident in the explosion of Internet of Things (IoT) devices (which will receive a further boost from 5G), proliferation of Application Programming Interfaces (APIs), super-fast software release cycles, as well as the continuous amount of new software written and deployed every year.

In parallel to our attack surface getting ever larger, data has become the new currency on the web, with cyber criminals targeting it in all its forms, from intellectual property to financial, health and personal data. At the same time, monetising data has become easier than ever, thanks to dark web marketplaces and cryptocurrencies. In the commercial world, artificial intelligence (AI), machine learning, and big data analytics have become indispensable in using, managing and monetising the ever-growing volumes of data.[4] New data privacy regulations, like the EU's GDPR and the California Consumer Privacy Act have been released to help individuals maintain control over their personal data, with whom they share it, and for which purposes.

In summary, IT is on a trajectory towards ever growing amounts of digitised data that is stored, processed and accessed by increasing numbers of computers, devices, apps and bots. The second major influence on the future of cyber security is its own history and how past security technologies and methods will shape the future. The following sub-sections shine a light on these "known knowns".

A perfect storm for defenders

We have a chronic talent shortage of more than 1.2 million cyber professionals. Most organisations report a lack of skilled cyber staff and consider this one of their top security concerns.[5] This situation is likely to further exacerbate in the coming years.

At the same time, the security industry is drowning in security products with an estimated 50 to 70 products for medium-sized organisations, and large organisations with more than 100 tools in use. This proliferation of tools implies that configuring, integrating, and operating security has become excessively complex and expensive. Historically, this situation was the result of decades of "defence in depth", where security products were layered on top of each other but never consolidated. There was also the failed idea that security could be achieved by enumerating and thwarting all threats and vulnerabilities, one at a time.[6] Secure development and the 'security by design' approach have emerged as a response to build inherently secure systems that need fewer bolt-on tools to protect them.

Meanwhile, cyber attackers continue to innovate by being both creative and pragmatic. Examples include developments such as ransomware, cryptocurrency mining, deep fakes, offensive (a.k.a. adversarial) AI as well as dark web value chains that support all activities needed to mount attacks.[7] Hackers seek out the weakest link in their targets, whether that's third parties and supply chain partners, unpatched systems, weak passwords, unprotected privileged accounts or humans who are susceptible to errors, phishing, social engineering, and insider threats. Many of the OWASP Top 10 vulnerabilities also remained surprisingly constant over the years, which further demonstrates a propensity for attackers to do "what works".

> "Data has become the new currency on the web, with cyber criminals targeting it in all its forms

> The traditional security model that everything inside an organisation's network should be trusted has been eroded

65%

of organisations have a shortage of cybersecurity staff

(ISC)² 2019

59%

of companies have experienced a data breach caused by a vendor or third party

Ponemon Institute 2018

Misplaced trust

The traditional security model that everything inside an organisation's network should be trusted has been eroded during the de-perimeterization movement. In 2018, 59 percent of companies experienced a data breach caused by one of their vendors or third parties[8] and the number of supply chain attacks had increased by 78 percent over the previous year.[9] 50 percent of today's attackers target not only their direct victims but all parties along the supply chain (called 'island hopping').[10] Beyond these headline numbers, supply chain attacks have been the root cause of many of the most significant cyber-attacks in recent years. No part of the digital supply chain has been spared, with attackers targeting commercial and open-source software, microprocessors, electronic controllers in cars, infrastructure services, outsourcing providers and the list goes on.

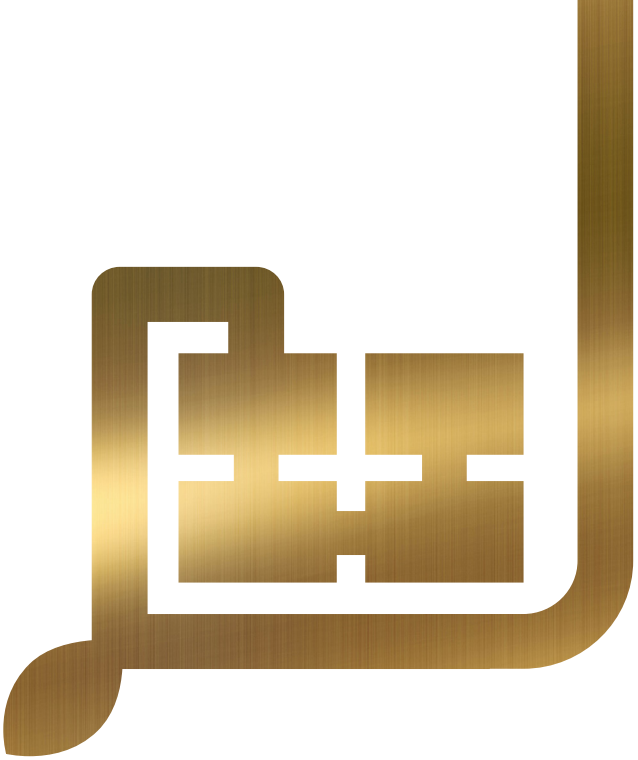
Responding to the threats arising from misplaced trust, Zero Trust Networks introduced a new design philosophy, according to which the amount of trust placed into any IT component should be minimized. This includes minimising the trust placed into hosts based on their network locations, trust in any host's ability to protect the data it stores, trust that input received from other applications is safe, trust in system configurations and third party code, and even trust in the physical environment. This is why Zero Trust advocates techniques such as encrypting data at rest, input and parameter validation methods as well as tamper proofing of exposed devices.

Counterintelligence

Computational propaganda, fake news, disinformation and 'influence operations' are spreading on popular social platforms and are purposefully amplified by algorithms to achieve unprecedented scale. Such attacks using IT systems (rather than against IT systems) have been used to shape election outcomes, geopolitical power, and corporate brand perception.[11]

The predominant 'defence-only' approach adopted by many organisations is not enough to deal with the current threat landscape. Therefore, a group of measures known as cyber counterintelligence have come into use to better anticipate, prepare for and respond to cyber-attacks. These measures include red teaming, threat intelligence, threat hunting, honeypots, sock puppets and deception.[12]

In summary, technology continues to become more omnipresent with an ever-increasing attack surface and attackers are combining creativity with pragmatism to break into IT systems. As defenders, we are experiencing a cyber talent shortage and the complexity as well as the cost of cyber security become increasingly unsustainable. To address these challenges, security models have been shifting and zero trust, security by design, and cyber counterintelligence have emerged as answers to improve security while reigning in cost, complexity and the dependencies on scarce talent.



Known unknowns

The known unknowns are the things of which we are aware, but do not understand fully. The most prominent known unknown is probably quantum computing. In simple terms, a quantum bit (a.k.a. qubit) can be both 1 and 0 at the same time, unlike traditional computing, which translates into an ability to perform multiple calculations simultaneously. Quantum computing will break or substantially weaken today's cryptographic protocols, we just don't know how fast this threat will materialise. Even assuming a 10-year time horizon, hostile actors could store encrypted data today with the objective to break it in 10 years' time. Moreover, the development of "quantum proof" encryption schemes requires years of research and engineering to deploy, which makes the quantum threat of great relevance, even today.

The COVID-19 pandemic also creates more known unknowns for the future of cyber security. COVID-19 has already started to accelerate digitisation. This can be seen everywhere from the rapid adoption of remote working, to online learning, e-commerce, new tools to track and report virus spread, remodelled supply chains, a growing preference for cashless payments, a boost in telemedicine, and even more cloud adoption. Seen through the lens of Business Continuity Management (BCM), 'digital' has become the fall-back plan for 'physical', which became unavailable due to social distancing requirements. The unknown factor is how far and fast society and business will drive digitisation.

The current wave of COVID-19-related phishing and social engineering attacks is likely to only be the first wave of cyber-attacks. Future waves will exploit less obvious vulnerabilities. For example, we are likely to see a peak in ransomware attacks as social distancing makes incident response difficult and victims are likely to pay more willingly. Work-from-home arrangements in emerging economies whose IT infrastructures are less well-equipped to support this will accentuate third-party cyber risks. Economically distressed companies are likely to be softer targets as they focus on keeping their business afloat, rather than excelling at cyber security. While the nuances of future attacks are still unknown, the general direction is clear.

The topics of resilience and crisis preparedness will emerge in an entirely new light from the COVID-19 pandemic. Many of today's systems are optimised for efficiency rather than resilience, which makes them fragile when circumstances change abruptly. Overnight, organisations and governments globally have discovered that they had critical dependencies on seemingly benign infrastructure components such as VPN networks for remote working, online shops, cloud-based video conferencing systems, as well as logistics organisations and suppliers of face-masks and other medical materials. This raises the broader question of what other dependencies we have in our IT systems, supply chains and geographic footprints, which should be reclassified as 'critical'. Once reclassified, new and heightened standards for security and resilience will apply and drive heightened levels of resilience throughout our operations. The direction is clear; the specifics are evolving.

The last known unknown is that COVID-19 will challenge us to decide how much privacy we are willing to sacrifice for the benefit of health and safety. News reports of tracking apps, monitoring of online chats, infrared surveillance cameras, and face recognition to detect transgressions in the use of face-masks have raised fears of expanding government surveillance that might extend beyond the immediate crisis.[13] If the 9/11 attacks are any indication, we can anticipate that surveillance will become a larger part of our lives and the extent to which privacy-preserving measures are employed is one of the unknowns for the time being.

51%

of cybersecurity professionals say their organisation is at risk due to cybersecurity staff shortage

(ISC)² 2019

Unknown knowns

Synthesizing the previous two sections, we now turn our eye towards the "unknown knowns", i.e. the hidden facts and untapped knowledge of which we are not quite aware, but we can derive by careful analysis. The only near certainty is that digitisation will continue its triumph and cybercrime will continue to innovate and grow. At the intersection of the trends and scenarios we've discussed, we arrive at the following conclusions for the future:

01

Cyber hygiene

Deploying foundational cyber security capabilities, or basic 'cyber hygiene' as it has been called, will remain a top priority as the security industry works to eliminate the known weakest links that still expose too many systems to cyber-attacks.

One indicator that cyber hygiene is getting better will be changes in the OWASP Top 10 vulnerabilities, which remained surprisingly constant so far.

02

Automation

Given the combination of talent shortages as well as increasingly complex and costly security solutions, automation and simplification become indispensable. Automation is helped by advances in AI and machine learning and cloud providers make significant contributions towards standardizing and automating security tasks. Already today, the quest for more automation has fuelled the success of security orchestration, automation and response (SOAR)[14] and we expect automation to become an increasingly important selection criterion in future security investment decisions.

> "The only near certainty is that digitisation will continue its triumph and cybercrime will continue to innovate and grow

03

Security by design

Rising further in importance, security by design will help eliminate more of the known weakest links and offer a viable solution to the ever growing digital ecosystem of IoT devices that cannot be patched. Cloud adoption also spreads the use of systems that are designed with security in mind and the Zero Trust philosophy discussed above is another instance of security by design. Lastly, less complex IT environments are easier to protect; therefore, driven by both cost and security considerations, CIOs everywhere are investing in the simplification of their IT infrastructures and application landscapes.

04

Counterintelligence

The aspiration to protect everything will continue to recede in favour of focused efforts that anticipate, detect and disrupt active threats. This approach is more labour intensive and requires experience to carry out activities such as the collection of relevant threat intelligence, compromise assessments or deceptive operations. Therefore, counterintelligence will be used primarily to thwart advanced threats as more basic threats should be covered by cyber hygiene, automation and security by design.

05

Recoverability

Recoverability is an element of cyber resiliency. The definition of cyber resilience is broad and includes everything from prevention to detection and response, and recovery. This has led to many organisations treating recovery as an afterthought, and the same holds for recoverability, i.e. the precautions that should be taken ahead of time to make the recovery from major cyber incidents faster and more efficient. We expect this to change and anticipate that recoverability will become a key design consideration on the same level of importance as prevention.

> "The history of cyber security has been one of evolution rather than revolution

06

(Self-)regulation

Following banking, pharma and electricity, more and more industries will be regulated, and regulations will get stricter and more prescriptive as governments conclude that IT security is too critical to be left up to business. Self-regulation will come in the form of stricter and stricter third-party controls that organisations will implement to protect themselves against potential cyber threats they import via their supply chains and third-party vendor relationships.

In summary, the history of cyber security has been one of evolution rather than revolution. Looking forward, continuity is therefore the most likely expectation and quantum computing is the potential disruptor that could fundamentally change how we defend our IT systems. Beyond quantum computing, security is likely to evolve according to the above six trends (cyber hygiene, automation, security by design, counterintelligence, recoverability and regulation) and in response to the trends and challenges outlined in this article. ■

Klaus Julisch
Lead Cyber Partner,
Swiss Risk Advisory

kjulisch@deloitte.ch

Endnotes

1. Max Roser and Hannah Ritchie (2020) - "Technological Progress". Published online at OurWorldInData.org. Retrieved from: https://ourworldindata.org/technological-progress.

2. Nick Davis (2019) – "Exponential Technology Trends That Will Define 2019". Published online at Singularity University. Retrieved from: https://su.org/blog/exponential-technology-trends-defined-2019/.

3. Gediminas Adomavicius Et al. (2019) – "The Hidden Side Effects of Recommendation Systems". Published by MIT Sloan Management Review. Retrieved from: https://sloanreview.mit.edu/article/the-hidden-side-effects-of-recommendation-systems/.

4. Rita Sallam Et al. (2019) - "Top 10 Data and Analytics Technology Trends That Will Change Your Business". Published by Gartner.

5. (ISC)2 (2019" – "Cybersecurity Workforce Study, 2019". Published by (ISC)2. Retrieved from: https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482.

6. Marcus J Ranum - "The Six Dumbest Ideas in Computer Security". Retrieved from: http://www.ranum.com/security/computer_security/editorials/dumb/.

7. Keman Huang Et al. (2019) - "Casting the Dark Web in a New Light". Published by MIT Sloan Management Review. Retrieved from https://sloanreview.mit.edu/article/casting-the-dark-web-in-a-new-light/.

8. Dov Goldman and Larry Ponemon (2018) – „Data Risk in the Third-Party Ecosystem". Published by Ponemon Institute.

9. "Internet Security Threat Report ", Symantec, Volume 24, 2019. Retrieved from: https://docs.broadcom.com/doc/istr-24-2019-en.

10. "The Ominous Rise of 'Island Hopping' & Counter Incident Response Continues ", Carbon Black, 2019. Retrieved from: https://www.carbonblack.com/global-incident-response-threat-report/april-2019/.

11. Chase Cunningham Et al. (2018) - "Zero Trust Outside The Wire: Combatting Cyber Influence And Espionage Threats". Published by Forrester.

12. Securitytrails Team (2020) - "Cyber Counterintelligence". Retrieved from: https://securitytrails.com/blog/cyber-counterintelligence.

13. Yuan Yang Et al. (2020) - "China, coronavirus and surveillance: the messy reality of personal data". Published in the Financial Times. Retrieved from: https://www.ft.com/content/760142e6-740e-11ea-95fe-fcd274e920ca.

14. Peter Firstbrook and Craig Lawson (2020) - "Innovation Insight for Extended Detection and Response". Published by Gartner.

Deloitte.