DXC.technology

White Paper

Security trends

Protecting the future

Table of contents

Prepare for another challenging year

DXC Technology is pleased to share our 4th annual cyber security state-of-the-industry report. Our aim is to highlight some of the disruptive trends that will have a profound impact on how we operate in cyberspace. Making predictions is complex—even more so when you mix the innovative and rapidly evolving digital landscape with a dynamic, relentless and creative adversary.

DXC Technology gathered some of the best minds in the industry, leveraging their years of experience to compile a balanced view of the challenges facing enterprises, governments, small and large businesses—as well as individuals and families.

The five trends included are not an exhaustive list but areas that we think will demand a concerted response by enterprises and nations. They are risks that will require a strategic governance approach, as well as an operational and technical response. This is an approach that we developed extensively with the World Economic Forum, which we will discuss later in the report.

These market trends focus on the evolving threat landscape. We discuss the dizzying scale of attacks, the worrying developments that bring human life into the cyber crosshairs, a breakdown of digital privacy and disclosure, the growing influence of a global cybercrime industry and the shortage of cyber security personnel.

We also share our view on how individuals and organizations can begin to respond to these risks. It is not enough to identify events; we must help build effective response mechanisms. Finally, the report looks at some of the emerging technologies we think will influence the cyber security world in 2017 and beyond.

We hope you find this report useful and informative. Stay safe.

Trend 1: Scale – Continued growth in the size and number of attacks

Our adversaries have learned to industrialize their operations, enabling them to perpetrate sophisticated and major attacks that were unimaginable just a few years ago. They now coordinate global attacks of a magnitude that can disrupt some of the digital world's fundamental building blocks.

A growing black market provides fast and easy access to existing malware, thus reducing the technical knowledge needed to launch damaging attacks. Crime syndicates are forming to leverage these off-the-shelf malware weapons. The trend is clear and sobering: Data breaches are growing in size and number, as illustrated by this online depiction of large-scale data breaches. We can expect that trend to continue in the coming years.

In September 2016, the cyber security site KrebsOnSecurity was hit by a massive distributed denial of service (DDoS) attack.[1] That same month, the Internet hosting site OVH was the focus of simultaneous distributed attacks totaling almost 1 Tbps (terabytes per second) in scope.[2] A month later, the Internet monitoring and routing firm Dyn suffered a massive attack that kept users from accessing Amazon, PayPal, Twitter, and other sites.[3]

When surveyed, a majority of business and IT leaders said their organizations saw as many or more attacks today as in 2014, and only 7% saw a decline in attack frequency.[4] Mandiant reports that in 2016, the company saw growing numbers of disruptive data-targeting attacks, that more breaches became public than ever before, and that the location and motives of attackers became more diverse.[5]

In the past we saw attacks on global companies and key government platforms. Today, hackers are also targeting small and mid-sized businesses, cloud vendors and other institutions. The sheer scale of those attacks, and the potential for widespread damage, will continue to grow.

After suffering what at the time was the second-largest attack in history, exposing 500 million customer accounts, Yahoo announced in mid-December 2106 that still-unidentified hackers stole data from more than 1 billion user accounts back in 2013.[6] That attack created real financial impact on one of the largest corporate mergers in history.

Attack surfaces are growing. Hackers will increasingly exploit the Internet of Things, the Industrial Internet of Things, web-enabled wearables, a growing universe of closed-caption TV cameras, obsolete firewalls and other devices capable of disrupting business or society.

Other areas of concern include mobile computing, email and web-based attacks, and the bring-your-own-device (BYOD) and bring-your-own-app (BYOA) workplace trends. As with other security trends, the nexus of identity and security will be crucial. The most common entry point, even for the largest attacks, is the individual user.

DXC guidance: The primary response must be to deploy collaborative defense systems shared by enterprises, governments and technology providers. What's needed is an in-depth defense that integrates 360-degree cyber assessments to understand threats and vulnerabilities and comprehensive measures to deploy prevention and continually monitor, detect and respond to threats.

Although a continued focus on perimeter-based network and infrastructure security is still needed, advanced tools—including biometrics, device-level identity controls, behavioral analytics, and machine learning—should also be deployed. Organizations must ensure that their defense and response capabilities are flexible and easily scaled. Many partner with trusted consultancies and service providers that offer advice and 24/7 real-time management of layered defenses with industry and geographical coverage.

A trusted cyber security partner

- DXC has over 4000 security consultants who advise, transform and manage leading-edge cyber capabilities, processes and technologies.
- Our network of global, intelligent Security Operations Centers (SOCs) enable us to deliver end-to-end security management and monitoring capability, 24/7/365, anywhere in the world. Sharing threat intelligence across multiple technology bases increases our ability to defend.
- We correlate billions of security events and manage more than 1.8M security-specific devices globally along with another 8M end-user and server devices worldwide.
- DXC Technology is the #1 independent pure play security services firm in the world.

[1] Forbes, September 25, 2016 - https://www.forbes.com/sites/thomasbrewster/2016/09/25/brian-krebs-overwatch-ovh-smashed-by-largest-ddos-attacks-ever/#5cceb53c5899

[2] Ibid

[3] Reuters, October 21, 2016 - http://www.reuters.com/article/us-usa-cyber-idUSKCN12L1ME

[4] 2016 Cyber Security Challenges, Risks, Trends and Impacts: Survey Executive Summary, MIT Technology Review in partnership with Hewlett Packard Enterprise Security Services and FireEye Inc.

[5] M-Trends Special Report, Mandiant Consulting, a FireEye Company, February 2016

[6] New York Times, December 16 2014, https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=0

Trend 2: Safety – Threats to people and critical infrastructure

Cyber adversaries traditionally have targeted customer data and financial assets. But with the expansion of the IoT, there is a growing threat to critical systems and industrial infrastructure, which poses a substantial risk to people. This increase in the number of devices means that any recall or update for security reasons will be far more complex and costly.

Cars are becoming rolling computer systems, offering a growing menu of consumer, business and fleet management capabilities. But since the 2015 hacking of an on-the-road SUV, connected vehicles and their associated security vulnerabilities have become the focus of recalls, legislation, and growing concerns.[7]

The medical device firm Hospira updated its infusion pumps with Internet-connected switches but did not add appropriate cyber defenses. The U.S. Food and Drug Administration later issued an advisory calling for hospitals to stop using the pumps, a sobering result for any company.[8]

In late 2014, the German government acknowledged a successful attack on a German steel mill. In the attack, hackers gained control of a smelting furnace and caused it to overheat, resulting in substantial damage to the furnace and interruption of the mill's business.[9]

Attacks against components of the Supervisory Control and Data Acquisition (SCADA) system architecture are becoming more frequent. The U.S. Department of Homeland Security's Industrial Control System Cyber Emergency Response Team (ICS-CERT) final incident response statistics confirm this growing threat. The number of incidents involving critical infrastructure grew 20%—from 245 in 2014 to 295 in 2015.[10]

As more networked devices are connected to the electrical grid, and with machine-to-machine automation, there is a growing concern about "cascades" of unintended effects across heavily engineered systems. And there are potential breakdowns across every part of society that depends on those crucial grids.

The consequences are clear: Operations can be slowed or halted, enterprise assets and reputation put at serious legal and regulatory risk, and consumers or citizens placed in serious physical jeopardy.

The engineered nature of IoT-connected and industrial control systems makes them well suited for digital security that leverages data, behavioral assessments and analytic intelligence. Going forward: Software and hardware vendors, managed security services providers, governments, law enforcement agencies and industry groups must collaborate to ensure a more secure IoT environment. We see more standards emerging and adapting to address this.

Trends continuing through 2017

- A shortage of cyber security talent
- Continued large-scale attacks
- Threats to critical infrastructure
- Disclosure of sensitive enterprise and political information
- Cyber-based extortion

[7] https://iapp.org/news/a/connected-cars-security-and-privacy-risks-on-wheels/

[8] U.S. Food & Drug Administration, May 13 2015, https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm446809.htm

[9] http://www.bbc.com/news/technology-30575104

[10] FY 2015 Year in Review, U.S. Department of Homeland Security, National Cybersecurity and Communications Integration Center/Industrial Control Systems Cyber Emergency Response Team

$7.7M

The mean one-year loss due to cyber crime among 252 surveyed organizations worldwide[1]

99 days

Median amount of time attackers spent inside organizations before detection[2]

86%

Of surveyed organizations that report a lack of adequate cyber security capabilities[3]

[1] 2015 Cost of Cyber Crime Study: Global, The Ponemon Institute, sponsored by HPE

[2] Hewlett Packard Enterprise, 2016 Cyber Risk Report

[3] Mandiant Consulting, M-Trends 2016 Special Report, February 2016

The U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework established a solid approach to protecting electrical grids, water treatment facilities, gas pipelines, tunnels, bridges and other infrastructure. The World Economic Forum offers frameworks and guidance for companies and governments that seek collaborative efforts to integrate cyber resilience into their organizations.[11]

DXC guidance: Organizations should look beyond the risk that cyber threats pose to their IP and confidential information. They now must consider the dangers posed to extended digital supply chains, the vulnerability of critical infrastructure, and the very real risk to customer and citizen safety.

Trend 3: Disclosure – Exposing sensitive enterprise and political information

Recent months have seen substantial growth in targeted and politically motivated attacks designed to affect or destabilize major organizations—including corporations and political institutions.

In previous years, this type of cyber activity was presumed but made far fewer headlines. Today we are seeing—and can expect to see in the future—more high-profile breaches, disclosures, doxing threats and hacktivism against nation states, political parties, companies and individuals. Recent incidents include cyber-attacks at the 2014 Sochi Winter Olympics, ongoing WikiLeaks disclosures and accusations of a hacking campaign to influence the 2016 U.S. elections—to name just a few. In 2017, politically motivated disclosures will continue, and we will see an increase in the level of public exposures against corporations.

On the enterprise side, executives once worried mainly about protecting intellectual property and confidential data. In the emerging cyber environment, companies are increasingly concerned with the disclosure of incriminating and embarrassing information.

Security firms continue to see shifts in the geographic and national location of adversaries, and in the balance of political and financial motivation for these attacks. Disclosure-based attacks will continue to tarnish global brands, influence and disrupt fair and legitimate processes—political and otherwise—and end once-promising careers.

DXC guidance: To address disclosure-oriented attacks in the future, organizations must deploy an integrated defense-in-depth solution that protects information, systems and people. Start by identifying informational assets that have economic or reputational value. Then make informed decisions about encryption, network segmentation, user rights restrictions and other measures needed to defend these reputational "crown jewels".

A robust, ready-to-launch and tested media and communications plan should be in place to support a rapid response to a cyber-based disclosure. Most organizations will have to use this at least once in the coming year even if just for internal communications.

[11] https://www.weforum.org/projects/partnering-for-cyber-resilience

Trend 4: Extortion – Monetizing cyber-based crime

In the rapidly expanding digital economy, identity connects digital systems to the physical world. Personal identity is the new security perimeter and the weakest link.

In 2017 and beyond, cybercriminals will continue to learn from the past—reverting to IP-enabled versions of the old-style "kidnap for ransom". Except that in the emerging Digital Economy, data is the hostage, payoffs are made in cryptocurrencies and other hard-to-trace methods and the threat is the destruction or exposure of critical or incriminating enterprise data.

In recent months, security firms have addressed a growing number of digital blackmail schemes. Attacks now target not only retailers and financial services firms but other industries, smaller firms, executives and individuals. Techniques vary from relatively simple phishing email methods to highly sophisticated spear-phishing attacks to deliver malware or ransomware payloads.

Attackers are increasingly using commodity ransomware, such as CryptoLocker, which is easy to find, buy and use. Once inside the enterprise, attackers demand ransom to prevent data destruction, public exposure, embarrassment and brand damage. Other malware locks users out of the system entirely. Consider a hospital suddenly denied access to patient health records—after which attackers demand cryptocurrency payments to decrypt and unlock the data.

Attacks are usually automated and often random, and when payments are made, they seldom make news. Not surprisingly, definitive research is lacking for this expanding threat; however, estimates project that damages from cryptographic file-locking attacks may have reached $1B in 2016. Mandiant reports receiving hundreds of calls from organizations and individuals whose files were encrypted with numerous ransomware variants.[12]

This threat will continue to grow. The crucial questions remain: After a breach has occurred and a ransom demanded, should organizations negotiate with attackers, and should they pay a ransom? DXC recommends caution in negotiation and payment of ransom. Such payments may be illegal in many jurisdictions. And of course, even if a ransom is paid, there is no guarantee the attacker will release the hostage data.

DXC guidance: First and foremost, establish and enforce a rigorous backup, recovery and business continuity program. Ramp up user training and awareness efforts, employ simulations to educate employees and test defenses, and consider deploying "honey pots" to trap and study attackers.

When you suspect an attack, first confirm a breach has actually occurred, then stay focused and carefully evaluate whether to engage an adversary. Law enforcement has encryption keys for some ransomware, and security services partners can help manage post-attack forensics and responses.

The best defense continues to be broad security training and improvements and engaging with experts before a criminal breach occurs.

[12] M-Trends Special Report, Mandiant Consulting, a FireEye Company, February 2016

Trend 5: Talent – A shortage of cyber security personnel

The talent war continues in IT security—between enterprises of all kinds, between the public and private sectors, sometimes between companies and their technology vendors, and certainly between the good guys and those on the criminal side of the cyber security landscape.

The simple fact is: The number of cyber security jobs available far exceeds the number of qualified professionals available to fill them. Through 2018, demand for cyber security talent will grow by 53%.[13] In 2017 and beyond, organizations will be measured against their competition based on their ability—or inability—to attract and retain cyber security talent. Gaps in those crucial capabilities will leave organizations dangerously vulnerable.

In one survey, 40% of business and IT leaders identified "lack of in-house expertise" as their single greatest cyber security challenge.[14] Between 2010 and 2015, cyber security job postings rose by nearly 75% and in 2015, more than 209,000 U.S. cyber security jobs were never filled.

Several factors are compounding the current talent shortage: the rapid evolution in the skills needed to be a top-class security professional; and the relentless need for continuing education, training and mentoring. Robust security capabilities require cyber data scientists and Internet of Things experts, further stressing the limited talent pool.

Staff turnover is another issue, as are burnout and a lack of clear career paths in many organizations. Experienced specialist talent is expensive and may only be needed for specific situations. As a result, many companies may be priced out of the market or find retaining these people too costly.

DXC guidance: Organizations should use creative recruitment, retention and reward programs. These can include hiring from outside traditional IT and security environments, leveraging innovative training and certification programs, and encouraging cross-functional collaboration. CISOs must engage their boards of directors in this vital discussion and shape career options.

Organizations can partner with third-party managed security services (MSS) providers to extend their security capabilities and use security consulting firms to define risk strategy to implementation plans for improving overall prevention, detection, risk response or management to define risk strategy to implement plans for improving overall prevention, detection, response or management of risk.

[13] Peninsula Press/U.S. Bureau of Labor Statistics

[14] Cyber Security Challenges, Risk, Trends, and Impacts Survey, MIT Technology Review, in partnership with Hewlett-Packard Enterprise Security Services and FireEye Inc., 2016

What’s next in cyber security technology?

As the headlines announce bigger attacks and growing costs, there is good news for enterprise security: Innovative security methods are emerging and existing tactics refined and extended. Security professionals can explore these and other advances in cyber security:

- Machine learning, artificial intelligence (AI), big data analytics and other advanced methods—including statistical models and adaptive rules to sort through gigantic volumes of data—are being refined to help identify the trace evidence of malware and other intrusions.
- Automated responses—leveraging more advanced techniques for security orchestration, incident investigation, containment and remediation—will help reduce post-breach dwell times and damage costs.
- Deceptive technologies, including honeypots and undercover surveillance, will increasingly be used to detect or deflect malicious attacks.
- Context-based analytics will be deployed to detect anomalies in user and network behavior and to counter adversaries who seek to circumvent traditional known and signature-based security methods.
- Purpose-built simulation environments with isolated networks are now being used to run the world’s most dangerous malware and to recreate actual attacks without allowing those malicious codes to spread.
- Segregation and containers are being refined to separate the security execution environment from the larger operating system, thus preventing OS attacks from compromising the security protections.
- New computing architectures are replacing traditional RAM- and disk-based storage with faster, nonvolatile memories. This allows security teams to process larger data volumes, find patterns faster and create new defensive techniques.

Other innovative technologies are being developed to more quickly detect anomalous network behaviors, to encrypt data even while it is in use, and to authenticate not only users and applications but also discrete processes and smart objects (IoT).

The importance of identity

Will 2017 be the year that identity becomes the single biggest cybersecurity concern? Today, identity is one of an organization's biggest targets, because having identity and passwords, adversaries can look across the organization. Looking forward, this issue not only increases in importance but also in scale as organizations increase the use of software as a service and cloud services, creating a need for hybrid identity. Special attention must be focused on identity in 2017 and beyond.

Digital credentials establish our identity in our corporate presence, e-commerce transactions, across social and communications networks, in hospitals, airports, and many personal and professional relationships.

One of the most vulnerable points in any business value chain is the human element. The adversaries know this, too. A hacked ID can open a cyber doorway into a financial institution, utility grid, member database or political party. In a recent report, 80% of all targeted attacks exploited privileged accounts during the attack process.[15] Thus, investigators find an identity component in virtually every major cyber security incident.

When an illicit activity takes place within a network, robust attribution is needed to understand who took the action and what they did. Our growing reliance on cloud, mobility and IoT technologies creates new and more vulnerable attack surfaces. We also exchange identity credentials with all these external services.

Going forward, to strengthen identity security, teams will need to employ robust identity-protection mechanisms. This will entail risk-based authentication and access, leveraging tools such as policy-driven adaptive authentication across multiple data points. Device fingerprinting will be used to more closely tie hardware to specific users. We will see increased deployment of behavioral analytics, biometrics, more responsive case management and stronger governance policies.

Protecting personal identities presents significant security challenges. Identity protection is decentralized in that all organizational resources have a part in ensuring protection. Training is key here to help educate employees and virtual employees (contractors, trusted partners, temporary workers) on the methods used by malicious actors and also the effects of compromised identities.

DXC believes that those who master identity will significantly increase their security resiliency and user satisfaction. Enhanced training throughout the organization and integrating new capabilities will help ensure identity validation. Creating a clear policy on hybrid identity is also required.

[15] CyberArk Threat Report: Privileged Account Exploits Shift the Front Lines of Cyber Security, CyberArk, November 2015

There's a lot at stake

As physical and digital worlds collide, the complexity, volume and variety of risks, threats and vulnerabilities continue to grow. The catastrophic effect of a cyber attack has a long-standing effect on an organization, its reputation, brand, shareholder value and consumer/citizen safety. No company, institution, individual or industry is immune to cyber criminals.

A 2016 report by MIT showed that less than 6% of business and IT leaders believe their organizations are "extremely well prepared" for security breaches. MIT also found that 42% of business and IT leaders say their organization's top executives do not understand what is needed to improve cyber security.[16] There is a real need to look beyond the traditional focus on security technologies, and to open a new and higher-level conversation about enterprise risk management.

Most organizations are at a crossroad in determining the best direction to move regarding their cyber security program. Digital transformation is upon us, IoT becomes increasingly more ubiquitous, and cloud and mobility projects continue to top the list of CIO and business leader agendas. All this combines to bring about tremendous new risks through the expanding variety of attack surfaces and work styles.

Many forward-looking organizations now view cyber security as a transformational enabler and as a strategic method to differentiate themselves to privacy-conscious consumers. The right security program can help organizations protect and accelerate key enterprise initiatives.

DXC believes that security is a leadership issue. Security must become a board-level conversation. And it should address the issues of identity management, governance, and the broader topic of enterprise risk management. Senior leaders need to turn their focus on enabling the CISO and security programs to combat the threats that increase every day.

Recognizing that cyber resilience is more a matter of strategy and culture than tactics, HPE (part of DXC) collaborated with the World Economic Forum and The Boston Consulting Group to develop a set of principles, frameworks, and tools that leaders can leverage to build cyber resiliency into their organization.[17]

It's easy to take a retrospective view and think of what should have been done, but looking into the future and trying to stay one step ahead of cyber criminals is no easy task. This paper brings together a set of risk factors that have a high probability of being top issues to contend with in the upcoming year.

[16] Cyber Security Challenges, Risk, Trends, and Impacts Survey, MIT Technology Review Custom, in partnership with Hewlett Packard Enterprise Security Services and FireEye Inc., 2016

[17] Advancing Cyber Resilience; Principles and Tools for Boards, World Economic Forum, in partnership with Hewlett Packard Enterprise and The Boston Consulting Group, 2017

Proven solutions to protect your digital enterprise and accelerate transformation

Cyber risk is one of the most critical challenges facing most boards, enterprises, countries and individuals. DXC is issuing this 2017 Security Trends report to highlight ongoing and developing tendencies in security threats, and to identify appropriate responses to those risks.

Given the serious nature of these threats, organizations cannot and should not try to go it alone. They should collaborate internally and externally to embed cyber awareness and capabilities into all aspects of the enterprise. Many institutions will choose a strategic cyber security partner to rapidly extend and augment their capabilities. Others will integrate solutions internally to meet their business needs.

Cyber threats pose very real risks to organizations and to the customers and citizens they serve. Now is the time to open the conversation and better understand security, risk management and how to protect your enterprise.

DXC Security Services partners with public and private organizations as they address the ever-changing security issues of 2017 and beyond. We provide security services for the digital economy, with end-to-end offerings to manage threats, costs and compliance.

DXC authors and contributors

Richard Archdeacon

James Cooper

Rhodri Davies

Ron Hardy

Chris Leach

Travis Lee

John Maynard

Jeff Misustin

Marco Pereira

Rob Stitch

George Tomic

Andreas Wuchner

Learn more at www.dxc.technology/security