Cyber Security Trends

A quick guide

This year, in an effort to drive awareness of cyber risks, we've created this short guide to explain the latest findings in cyber security. Continue reading to learn about key threats, leading causes of data leakage and more.

Cyber criminals have a varied and growing portfolio of techniques for gaining access to organisational resources and for obtaining control of systems. Their strategies include, but are by no means limited to, the following:

- Manipulating personnel with social engineering techniques
- Exploiting potential vulnerabilities in websites and web applications
- Attacking network technologies and anything with a connection to a network

In order to meet these challenges, organisations need to develop an integrated approach to managing their technology, processes and people. To be proactive, organisations must understand the vulnerabilities that leave their infrastructure and applications exposed, as well as the measures necessary to close any gaps in their security.

Top findings about cyber risks

Organisations are failing to cover the cyber security basics.

THE TOP 10 EXTERNAL VULNERABILITIES ACCOUNTED FOR NEARLY 52% OF ALL IDENTIFIED EXTERNAL VULNERABILITIES.

THOUSANDS OF VULNERABILITIES ACCOUNT FOR THE OTHER 48%.

(source: 2016 NTT Group Global Threat Intelligence Report)

Why does it matter?

The prevalence of common vulnerabilities highlights that many organisations lack basic cyber security measures. Hackers can exploit these vulnerabilities to attack the majority of organisations and their systems.

Criminals have a long list of attack methods to choose from. However, some types of attack are more common, and knowing which ones they are can make it easier to prioritise your cyber defences.

Something as simple as applying available updates for operating systems and applications such as browsers, plugins and desktop apps could prevent these basic vulnerabilities. These updates include both security and feature patches, and are meant to fix or improve the software you use.

Exploit kits continue to threaten organisations' defences.

EXPLOIT KITS ACCOUNT FOR 40% OF THE MOST COMMONLY ENCOUNTERED EXPLOITS.

(source: Microsoft Security Intelligence Report, Volume 16)

Why does it matter?

Hackers have a monetary incentive to improve results and efficiencies. This makes exploit kits particularly attractive to attackers. 2016 saw dramatic changes in the exploit kit environment. At the start of the year, Angler, Nuclear, Neutrino and RIG were the leading exploit kits. By November, RIG was the only one from that group still active.

Now that three of the most dominant exploit kits have left the field, smaller players and new entrants can expand their market share. Cisco advised that exploit kits that appeared poised for growth in late 2016 were Sundown, Sweet Orange and Magnitude. These kits, as well as RIG, are known to target Flash, Silverlight and Internet Explorer vulnerabilities (Cisco 2017 Annual Cyber Security Report).

People are the weakest link when it comes to cyber security.

Privilege abuse is the leading cause for data leakage determined by malicious insiders.

(source: Verizon, 2016 Data Breach Investigations Report)

Why does it matter?

Privilege abuse – accessing information for unsanctioned uses – is the leading way in which data is leaked by malicious insiders.

Organisations need to monitor authorised daily activity, especially that of individuals with access to sensitive data. You also can't effectively protect your data if you don't know where it resides. Ensure that you're aware of exactly where your data is, and be careful who you give privileges to and to what degree.

Phishing costs businesses.

85% of organisations have suffered phishing attacks.

Two-thirds of organisations reported experiencing attacks that were targeted and personalised (spear phishing), up 22% from the year before.

(source: Wombat Security Technologies, The State of the Phish 2017)

Why does it matter?

In 2015, Ponemon Institute reported that lost employee productivity is the largest cost associated with phishing, at roughly $1.8M for a 10,000-person company (Ponemon Institute, Cost of Phishing and the Value of Employee Training).

Cyber criminals are focusing on more sophisticated endeavours that can provide higher rewards, like spear-phishing attacks. It is estimated that the profit from a spear-phishing attack can be more than ten times that of a mass attack (Cisco 2017 Annual Cyber Security Report).

Phishing plays on human vulnerabilities and that's why any comprehensive plan to combat phishing must start by educating employees about the role they play in the organisation's overall information security posture. The best defence against phishing is a continual, hands-on training programme.

The ransomware business is still booming.

NEARLY 50% OF ORGANISATIONS HAVE BEEN HIT BY RANSOMWARE.

(source: Osterman Research, Understanding the Depth of the Global Ransomware Problem, 2016)

Why does it matter?

According to a June 2016 survey from Osterman Research, almost one out of every two participants indicated their organisation had suffered at least one ransomware attack in the past 12 months.

Of the IT professionals surveyed by Barkly who had experienced a ransomware attack, only 42% reported being able to successfully recover all their data from backup.

Emails with malicious links and malicious attachments account for 59% of ransomware infections. According to the Osterman Research report, users are more than twice as likely to be infected by clicking something in an email than by visiting an infected website directly.

The risk from OAuth connections is growing amid an app explosion.

27% of connected third-party Cloud applications introduced by employees into enterprise environments in 2016 posed a high-security risk.

(source: Cisco 2017 Annual Cyber Security Report)

Why does it matter?

Applications create a risk for enterprises. They connect with the corporate infrastructure and can communicate freely with the corporate Cloud and software-as-a-service (SaaS) platforms at the point that users grant access through open authentication.

Growth is explosive. There were about 129,000 unique applications observed at the beginning of 2016. By the end of October that year, the number had grown to 222,000.

CloudLock categorised the risk level of 222,000 applications used by 900 organisations. Of those total applications, 27% were deemed to be high risk, while the majority fell into the medium-risk category (Cisco 2017 Annual Cyber Security Report).

Netskope found that 66.3% of all Cloud service providers lack the proper security, privacy controls and industry certificates to comply with the General Data Protection Data Regulation (GDPR).

Shadow IT is a threat to security.

80% of end users use software not cleared by IT.

(source: Cisco, The Shadow IT Dilemma)

Why does it matter?

Company personnel are increasingly introducing new risks with workarounds for legacy IT solutions.

In small and large enterprises, personnel gravitate towards the simplest solutions. Legacy methods can be slow and may not work as well for employees on the go. Why waste effort finding and requesting a work-sanctioned application when your mobile or tablet is sitting on the table?

Shadow IT presents a serious risk to businesses. Each additional unsanctioned device or application increases the organisation's attack surface and increases the likelihood of information mismanagement.

Using the Cloud expands an organisation's security perimeter.

The average number of Cloud-based applications in use has nearly tripled in the past three years, from 545 in Q3 of 2013 to 1,427 in Q3 of 2016.

(source: Skyhigh, Cloud Adoption & Risk Report)

Why does it matter?

Security professionals who participated in Cisco's third annual Security Capabilities Benchmark Study cited mobile devices, public Cloud, Cloud infrastructure and user behaviour as top sources of concern when they think about their organisation's risk of exposure to a cyber attack. This is understandable. The proliferation of mobile devices creates more endpoints to protect.

The Cloud is expanding the security perimeter. And users are, and always will be, a weak link in the security chain.

Organisations must:

- Integrate their security technology
- Simplify their security operations
- Rely more on automation

This approach will help reduce operational expenses, ease the burden on security personnel and deliver better security outcomes.

The supply chain presents a risk to cyber security.

On average, only 35-57% of partners were vetted, placing most enterprises at considerable risk.

(source: Accenture: The State of Cybersecurity and Digital Trust 2016)

Why does it matter?

Despite a majority of enterprises either currently vetting or planning to vet ecosystem partners for cyber security capabilities, enough gaps exist to be of major concern. To highlight the scale of the risk, 63% of breaches can be traced to third-party vendors, according to Soha System's survey on third-party risk management.

Security professionals must convince executive management that improved vetting of partners is essential by reviewing third parties' data safeguards, security policies and procedures, and determining whether their security posture is sufficient to respond to a data breach or cyber attack.

Budgets are the biggest obstacle to security.

35% of security professionals said that budget was their biggest obstacle.

(source: Cisco 2017 Annual Cyber Security Report)

Why does it matter?

In 2016, 35% of security professionals said that budget was their biggest obstacle to adopting advanced security processes and technology.

However, budgetary constraints are only a contributing factor. Compatibility issues highlight the problems of disconnected systems that don't integrate, and concerns about the lack of trained personnel highlight the problem of having the necessary tools but not the skills to understand what is happening and how to react.

Security professionals will have to evidence the need for better cyber security. For example, when it comes to finance, security teams must compete against many other corporate priorities. If they can't secure funds for more tools, then the budget they do have must work harder. For example, automation can be used to offset limited manpower.

Security professionals are forced to ignore security alerts.

54% of legitimate alerts are not remediated.

(source: Cisco 2017 Annual Cyber Security Report)

Why does it matter?

Maybe because of the reasons stated previously — such as a lack of tools or resources – organisations are reporting that they can only respond to half the security alerts they receive in a given day.

To investigate and understand a greater percentage of the identified alerts, organisations need to rely on automation as well as invest in appropriate tools. Automation can help free up resources and remove the burden of detection and investigation from the security team.

Conclusion: an expanding attack surface requires an integrated approach.

Defenders must take a more proactive stance to stay ahead of basic attack tactics. Security teams should be:

- Conducting regular staff training and awareness programs
- Gathering information about the latest threats and vulnerabilities
- Ensuring they are controlling access to their networks
- Limiting their organisation’s exposure
- Managing configurations
- Developing consistent response practices and procedures

By following this approach, security professionals will be able to take the necessary preventive measures to reduce the threat of attacks, and to inform senior management about possible exposures and vulnerabilities.

Our technical services

CYBER ESSENTIALS CONSULTANCY AND CERTIFICATION	PENETRATION TESTING	PCI DSS CONSULTANCY AND COMPLIANCE	IT HEALTH CHECK	TRAINING AND KNOWLEDGE TRANSFER
Prove that you take security seriously. IT Governance's fixed-price solutions can help you achieve certification to either Cyber Essentials or Cyber Essentials Plus at a pace and budget that suits you.	Forewarned is forearmed. Test your defences with our penetration testing services. By simulating an attack, we can detect your business-critical vulnerabilities and work with you to protect your systems.	We cover the entire range of payment card compliance services. As an authorised QSA company, we will assess your needs, explain the PCI compliance requirements, and provide solutions that will suit your budget.	IT Health Checks are designed to provide you with a complete view of your system's strengths and vulnerabilities from an unbiased, expert perspective. Our health checks can be customised to your needs.	Training courses for all staff, IT practitioners and lead implementers seeking to implement various standards, including ISO 27001 and the PCI DSS, as well as professional certifications like CEH and CISSP.
Find out more	Find out more	Find out more	Find out more	Find out more

Our company

IT Governance is the world's leading global provider of IT governance, risk management and compliance solutions. Our comprehensive range of products and services, combined with flexible and cost-effective delivery options, provide a unique, integrated alternative to the traditional consultancy firm, publishing house, penetration tester or training provider.

Speak to an expert

Please contact us for further information or to speak to an expert.

T: +44 (0)845 070 1750

E: servicecentre@itgovernance.co.uk