Business white paper

Get prepared

Cyber security predictions

Table of contents

Plan for the worst; fight for the best

Combatting cybercrime requires an integrated security approach, incorporating proactive planning and risk management strategies to lower risk exposure, reduce security-related costs, and gain greater control. It's time to invest more in prevention and real-time threat detection for the application layer, and hardware and software interface.

Every action in the physical, business, and interpersonal world is increasingly transacted, captured, and reflected in digital form. This increases the new challenges being faced—ranging from storing, securing, and managing information, to the bigger challenge of how to extract value from it whilst guaranteeing privacy, security, and data ownership.

The (r)evolution of cyber security

The digitisation and interconnection of society, and, in particular, critical infrastructures, increase the risk of accidental or deliberate cyber disruptions. International cyber criminals go unpunished and an escalating cyber arms-race threatens global and regional stability. Let's look at the trends and predictions for cyberspace over the next 18 months.

The threat is real

There are tectonic shifts occurring in cyberspace, from mobility to wearable technology. Those shifts drive even larger changes in the threat landscape and in how enterprises respond. The potential impact of cyber-attacks and disruptions is increasing due to continuing digitisation of existing business models and adversary groups' desires to disrupt information flows. The lack of technology sustainability and increasing connectivity are now frequently seen as a threat to society and enterprises. CEOs and business leaders recognise the importance of cyber risk and managing breaches in an effective manner. Digital privacy is now a major topic in most nations, and organisations are under pressure to regulate data collection and surveillance.

Predictions through 2016

- Major mobile exploits
- Open-source vulnerabilities
- Compromised supply chain
- Industry-sector attacks
- Increased privacy pressure

Evolution of the adversary

Cyber activity levels will continue increasing, and more and varied players will become involved. Cybercrime affects 378 million victims per year, with an average of 12 users falling victim every second of every day. At an average cost to each individual of $298, cybercrime has become much more than a nuisance. For companies, the average cost of cybercrime is staggering, at a whopping $7.4 billion (USD).[1] We also believe this number to be significantly under reported, due in part to the sensitivity of reporting and the negative impact to brand reputations.

It's clear that cyber criminals have evolved drastically over the past decade. These days, they join forces in an online marketplace where they share and sell tools, tactics, and targets—all aimed at stealing financial information, intellectual property, and private data. These online adversaries specialise around different facets of the cyber-attack chain; working together to create, share, and act on security intelligence to exploit organisations.

Uncertain cyber leadership

Research, done by HPE in tandem with The Economist Intelligence Unit, found that only 33% of CEOs have a single view of information risk across their organisation, and only 28% were able to attribute a monetary value to their information assets.[2] Such a limited view should drive organisations to step back and assess the state of their defences, and, if necessary, launch a full security improvement programme that might include capability maturity assessments, cyber-risk profiling, and incident-response planning.

[1] Ponemon: Cost of Cyber Crime Report, 2015

[2] Information Risk: Managing digital assets in a new technology landscape, The Economist Intelligence Unit Limited, 2013, **http://www.economistinsights.com/sites/default/files/EIU%20information%20risk%20white%20paper%20-%20managing%20digital%20assets%20in%20a%20new%20technology%20landscape%20WEB.pdf**

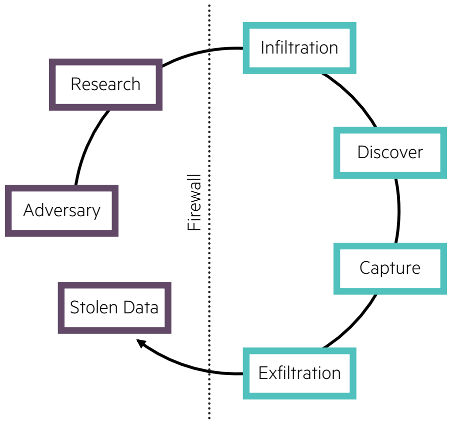

Figure 1: The adversary attack ecosystem

79%

of senior business leaders said executive- or board-level involvement is needed in the incident-response process in a recent HPE and Ponemon Institute survey. However, there is widespread disagreement about how that involvement should take shape. Only 44% rated their breach response plan as mature and proactive.[3]

Recent high-profile attacks, regardless of who's responsible, indicate the extent to which even mature organisations are ill prepared, and senior executives can be embarrassed. Improved response, especially at the executive level, is required.

However, this does not bode well with the skilled manpower shortage, now a trend in the security market. In fact, in a recent study from HPE and Frost & Sullivan on adoption trends for Managed Security Services, 52% of the respondents identified staff shortages and insufficient training as primary impediments to effective security management.[4]

In short, organisations need to think innovatively as to how services and capabilities will be delivered and by whom.

Predictions tied to trends

Every organisation is different in its own way, but all operate within the broader cyber-threat landscape and face similar challenges doing business in the digital economy. The advent of the collaborative threat market place, where sophisticated actors share best practices and hone their attacks, should be a wake-up call for organisations globally. Organisations are stimulated to act, but many continue to "go it alone" with reactive strategies. In doing so, the risk to those organisations grows. However, by building scenarios about what may happen, organisations and their security partners can model the threat response and address key risk areas.

Trend 1—Major mobile exploits

Mobility is not only a fact of life in today's enterprise—it can be a key competitive advantage. Yet, it brings unique security challenges that combine technical, behavioural, and operational aspects. There are a number of trends flowing together that make it more likely that the next 18 months will see an increase in mobile-based breach incidents. The line between work and personal life is evaporating as enterprise and consumer experiences continue to meld. The average person moves between three to five personal devices throughout a day, including laptop, smartphone, and tablet. Now, with the introduction of wearable technology, the sensor—such as augmented reality smart watches/bands, and smart home energy/home entertainment, there's even more to secure.

Additionally, an increasing number of vulnerabilities have been discovered in Android-based systems, exposing additional attack points and complicating support. There hasn't been a major mobile breach yet, but it's only a matter of time. In 2014, for example, Android saw targeted attacks using mobile devices on iOS. There was also the start of attacks on mobile cloud services, with a celebrity photo-hacking scandal attracting significant attention.

[3] Ponemon, "Cost of Cyber Crime Report," October 2014

[4] HPE and Frost & Sullivan, "The HP Global 2015 State of Managed Security Services Report", July 2015

This trend won't bypass cyber adversary groups; 2015 may be the year of mobile spear-phishing and mobile Advanced Persistent Threats (APTs). New mobile functionality and form factors will make them a potential route to greater riches than can be delivered from just the device. Personal health information, geolocation, e-wallets combined with near-field communications, wearable integration, online payment systems, and access to cloud data or corporate applications create a lucrative and high-risk information store to exploit.

Contactless payment systems also offer potential growth areas for attackers as a financial target. The increasing number of devices attached to increasingly complex networks, often out of an organisation's direct control, will provide more entry points to targets that matter.

Recommendation: Know how users in your organisation want to use their devices and ensure they understand the security issues. Also, make sure they're protected with basic defences such as strong passwords and the correct endpoint protection. Consider enterprise identity and access gateways to enforce corporate polices whilst supporting consumer choice.

Trend 2—Open source vulnerabilities

65%

of companies that reported sharing customer data with a partner also reported a subsequent breach through that partner.[5]

During the last 12 months, vulnerabilities were found in key applications and functions based on open source software—Shellshock and HeartBleed come to mind. The most common vulnerabilities will still be found amid the main commercial software vendors' products. But, as their response to security becomes stronger, adversary research for vulnerabilities in softer target areas will increase. We have seen zero-day vulnerabilities increase over the past few years, expanding from traditional commercial off-the-shelf software to open source code that has become part of many organisations' infrastructure—from Linux® Kernel, to GNU Utilities, Apache, and MySQL.

Typically, businesses turn to open-source software as it's generally free, continually evolves in real time, avoids vendor lock-in, and can be easily adapted. It does, however, have some disadvantages versus proprietary software, which focuses on usability, documentation, governance, and support. The major disadvantage with open systems: Many people identify bugs, and malicious users can exploit these vulnerabilities.

Recommendation: It's important organisations understand where they use open-source software and identify the significance to their business. This may require a refresh of your policies—on use, implementation, and software updates. Where a risk is identified, but not clearly defined, additional application and vulnerability testing should take place—especially when an Internet-facing function is involved.

Trend 3—Supply chain will remain a critical attack vector

Cyber criminals typically look for the weakest link—the most efficient, easiest way into a system; the majority of the time, suppliers are the easiest way in. Remember the headline-grabbing data breaches involving Target, AutoNation, Lowes, and AT&T—all have been linked to their trusted third-party vendors as the origin of compromise.

The sheer breadth, scope, and interconnectedness of the global supply chain severely hampers efforts on the defenders' side. By its very nature, it's highly fragmented. Large enterprises are getting better at security, so criminals are turning to their partners' networks instead. Generally, these organisations have fewer security controls, making them easier to exploit. They also hold network credentials that can be stolen.

Contracts of all sizes have risks associated with sharing information. And all suppliers share information with their vendors. Even if the contract is with a small supplier for an indirect category, it carries risk. So can a top-10 critical suppliers list—even if you make sure they're secure; that list might change or grow, or some random website created by a third party that wasn't in the top 10 may be the risk.

[5] Ponemon Institute: "Cost of a data breach study", 2014, **http://info.hpenterprisesecurity.com/LP_CP_424710_Ponemon_ALL?src=Securityweekemail**

Recommendation: Enterprises, like yours, must consider the security governance and compliance policies of their suppliers as a key component of their overarching enterprise security approaches, including annual reviews, enforcement, and reporting. Current governance programmes may require adding staffing or even outsourcing to accommodate increasingly extended supply chains.

Trend 4—Industry-sector attacks and malware

Over the past few years, we've seen ever-increasing adversary specialisation in attackers' techniques and targeted companies. An example of this was Dragonfly in 2014. This was a concerted campaign to target hundreds of energy companies in North America and Europe. It included a range of sophisticated and blended attacks aimed at organisations that use industrial control systems to manage electrical, water, and oil and gas systems.

Those planning attacks will aim at the easiest and most lucrative targets to maximise their opportunity. The more detail around an individual profile, the greater the information's value, the better the return on investment. Criminal gangs specialise in particular industry sectors and supply chain elements. Those with healthcare information, just like those in retail, hold a wide range of information around an individual, which makes them attractive to attackers. The market for credit card data will mature into one offering individual profile data. Groups of credit card data are now being categorised into region/ZIP code and sold to maximise the time value of the stolen credentials.

Even sectors such as transportation are proving tempting, with particular focus on loyalty programme data and self-service check-in kiosks as sources of valuable user data. Most ports and terminals are managed by industrial control systems, which have, until very recently, been left out of the CIO's scope. Historically, this security hasn't been managed by company CISOs, and maritime control systems are very similar. As a consequence, improvements that many companies have made to their corporate cyber security to address the change in the threat landscape over the past three to five years haven't been replicated in these environments.

Recommendation: Ensure all defences that already exist meet your organisation's needs and provide the best brand protection possible. Start with assessing physical and operational security stakeholders. Adopt measures from leading sectors, for example, financial and retail, and adopt a continuous monitoring approach.

Today, it isn't just the traditionally high-value industry sectors of financial services, telecommunications, and transportation getting targeted. There's a new wave of sector-specific attacks and malware aimed at transportation, business process suppliers, healthcare, and manufacturing.

- **Finance and banking**—The finance industry is one of the main target pillars of cyber security. Due to the industry's nature, the lucrative sector lures hackers and cyber criminals originating from multiple disciplines throughout the world, some of which are either crime syndicates or well-founded organisations.
- **Telecom and media**—Telecom and media organisations hold the foundation and the infrastructure facilitating data communication on the planet. From wireline to wireless communication, these services need special protection that emerged in the cyber decade and have constantly evolved ever since.
- **Critical infrastructure**—Protecting critical infrastructure elements becomes a key factor in industrial control system (ICS) defence strategies. SCADA and DCS systems govern the logical to physical elements that control our daily lives.
- **General IT**—Today, the ever-changing and evolving technologies trends and threats present new challenges for organisations with any IT infrastructure.

Trend 5—Privacy concerns drive greater legislation

As governments grapple to improve cyber-security maturity and manage data privacy across domestic and sometimes geo-political digital landscapes, regulation and oversight are on the rise. In the last 12 months, nation-state attacks and related disclosures led to a number of governments taking a stronger interest in security and privacy issues.

Specific legal requirements—for specific vertical industries such as power and energy, and healthcare—now have to be implemented, bringing them in line with the pressures that have existed for the financial sector for some years.

The public mood is also changing; increased use of technologies such as cloud processing and storage requires a greater understanding and clarity of jurisdictional boundaries and the ability to clearly express these to customers and regulators. The Internet of Things (IoT)—everything connecting to everything via the Internet—will drive even more sources of individual data capture, for example, the rollout of ubiquitous solutions such as smart metering.

A recent report by the BBC in the UK showed online privacy as being one of the highest topics on the political agenda for first-time voters.[6] This trend is also appearing in the U.S., where recent polls show that more than 90% of Americans think that consumers have lost control of their personal data.[7] This will drive even more political attention to this topic.

[6] BBC, "General election 2015: Youth vote 'could be key to win,'" Dec. 29, 2014, **http://www.bbc.com/news/uk-politics-30620164**

[7] Pew Research, "Public Perceptions of Privacy and Security in the Post-Snowden Era," November 2014, **http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/**

Recommendation: Understand what individual data is held through privacy assessments to ensure you have a robust data-loss prevention capability in place. The applications that access and process data will need consistent testing routines. Also, assess and understand your data "crown jewels"—don't just let compliance drive data protection. Understand and take advantage of suppliers' Safe Harbour agreements to not overly complicate global operations and risk overlooking real security needs.

IoT—Connected consumer/person. Connected home. Connected with existing stakeholders. To ensure security, assess early projects, and embed "enterprise view" for risk management early in project lifecycle.

Good news—there are answers

It's not all doom and gloom as new defence capabilities come to the forefront. So perhaps the biggest challenge or opportunity that security professionals face is understanding these and ensuring that the need is reflected in future budget cycles, including investments in strategy, design, and skills acquisition.

Security intelligence continues to grow, and the concept of trust between parties is being automated. Being able to share intelligence data on attacks between specific parties such as a group of similar organisations in the same vertical must be a priority.

Big Data and automated analysis will become increasingly available to identify the most subtle APT. This is needed to cope with the huge increase in scale created by the sheer growth in users, attack vectors, and targets.

Cooperation and collaboration between security players will start and enable linked-up services. More of these will be based in the cloud, enabling more rapid and scalable deployments through integration and automation.

New technology solutions are gaining traction; this provides greater insight into who's logging in and using your data. This, when combined with the capabilities provided by Big Data, will enable organisations to identify errant users with greater granularity and speed—by using fraud and behavioural analysis.

Technologies to watch into 2016
"Signatureless" APT and anti-malware technologies are getting more and more mature. Besides their current network and desktop/notebook focus, they are now extending into the mobile space. With dramatic trends toward IoT, more and more security technologies and services are moving into the cloud. Instead of having them locally installed, they'll more likely be consumed as a Service. From a technology point of view, the technologies used aren't necessarily new, but they're getting virtualised and made available from everywhere. The business model is also changing with a focus toward pay for use.

In the identity and access management (IAM) arena, there's a similar move toward cloud. With the New Style of Business, and a focus on mobility and cloud, IAM services are shifting and enabling companies to provision and manage identities within all these platforms. The technologies used are not totally new; they're adapting to the new challenges of the innovation economy.

Final prediction: Enterprises and governments will have a constant demand for increased and better managed security.

HPE Enterprise Security—the solution

HPE Enterprise Security focuses on securing future agencies and enterprises in the ever-evolving connected world. We are committed to enhancing defences against the many evolving cyber threats to governments, individuals, commerce, and critical global infrastructure by developing international standards, policies, and legislation that encourage outcome-based approaches to cyber security.

HPE Labs is leading major new research that addresses how cloud service providers use and protect personal and confidential information in the cloud. Our TrustCloud project addresses key issues and challenges in achieving a trusted cloud environment. In addition, under the Dynamic Defense research project, HPE Labs also tackles the application security problem by developing technologies that present a constantly changing surface to attackers, limiting their ability to detect and exploit vulnerabilities.

The HPE cyber-security capability covers 67 countries across all industry verticals. Our 5000 security professionals manage more than 10,000 enterprise clients and see 100 billion security events each month. HPE security research identifies more zero-day vulnerabilities than anyone else[8] and has a community of 2800 cyber researchers globally. Our 10 Global Cyber Security Centers enable us to deliver an end-to-end security capability anywhere in the world and share threat intelligence instantaneously. At HPE, we have over 1000 security consultants who advise, transform, and manage adoption of new cyber capabilities, processes, and technologies.

[8] **https://community.hpe.com/t5/Security-Research/ZDI-10-10-fascinating-facts-about-10-years-of-bug-hunting/ba-p/6770127#.WBMOAWbrtaR**

HPE Security Research publishes free security summary briefings available to the public on our website and iTunes, which provide the most current security intelligence available. HPE also launched the Threat Central Partner Network, where a collection of like-minded companies share cyber intelligence with the larger community to identify and stop attacks before they start.

About the author and contributors

Andrzej Kawalec
Andrzej Kawalec, chief technology officer, Enterprise Security Services, HPE, is responsible for information security strategy, solutions, portfolio, and market-facing activities. Kawalec leads a global research and innovation team that focuses on cloud, consumerism, cyber security, and business risks surrounding information security systems, policies, users, and processes. A recognised leader in security and business-continuity planning, Kawalec is a frequent speaker at industry events.

Richard Archdeacon
Richard Archdeacon, chief technologist, Information Security Strategy, HPE, leads the development of new strategic concepts and solutions in the cyber market. He came to HPE with 25 years of experience in consulting with major corporations across Europe, the Middle East, and the U.S. Archdeacon served on the IAAC board and IISP Accreditation Committee, and holds an MBA from Cranfield University. He is currently an industry advisor to Coventry University for their new MBA programme in cyber security.

Simon Ian Arnell
Simon Ian Arnell, chief technologist, Research and Development, HPE, worked within the Enterprise Security Services organisation in pre-sales, delivery, innovation, and thought-leadership capacities. He frequently hosts C-level clients at our HPE Labs Executive Briefing Center, enabling him to validate research and development concepts with services previews and pilots. Arnell architected a number of enterprise security services and filed a number of supporting patents in security software, security Big Data analysis, and software-defined systems.

Rhodri Davies, PhD
Rhodri Davies, chief technologist, Managed Security Services, HPE, specialises in designing security services. Davies works with a variety of HPE client organisations—large and small. He examines how they currently manage information security and gives them advice on how to best protect themselves in the future. Prior to entering the commercial sector, Dr. Davies worked as a post-doctoral researcher at the University of Manchester in the United Kingdom.

Andreas Wuchner
Andreas Wuchner, chief technologist, Security Innovation, HPE, is a recognised practitioner with 20 years of experience in information security, IT security, and IT-risk management. Before joining HPE, Wuchner was the CIO security technology and a managing director for UBS in Switzerland, where he also served as group information security officer (GISO) and head of IT Risk Control within the bank. He has a master's degree in electronics and computer science from the University of Applied Sciences in Offenburg, Germany.

Learn more at
hpe.com/services/security

Sign up for updates

Hewlett Packard Enterprise

4AA6-0910EEW, October 2016, Rev. 2