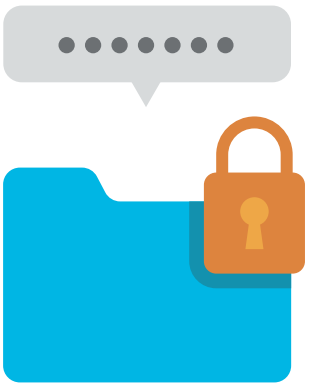
Business white paper

Security Begins at the Endpoint

The case for prioritising endpoint security

Brought to you by

Executive Summary



82% of organisations have experienced a cyber security threat/breach in the last 12 months.[1] Cyber crime is increasing in attack frequency, severity and cost.

The paradigm of prevent and protect security – defending a firewalled network perimeter – is over. Detect and respond is far more effective.

But IT budgets are failing to keep up with the changing face of cyber security. 77% of spend is still in prevent and protect.[2] Only 36% of IT security managers feel they have ample budget for effective endpoint security.[3]

Robust data protection is possible. With the right technology – from detect and respond security solutions down to individual devices – the right strategy and enough resources, organisations can protect themselves from cyber crime.

Failure to increase investment in cyber security, and to realign investment towards truly effective defence, will result in an increased frequency of security breaches - at an increased cost to the organisation.

Introduction

Cyber security in the age of amorphous networks
60% of IT leaders feel the increasing volume and sophistication of cyber crime is outstripping their defences. 80% of security leaders perceive the threat from Advanced Persistent Threats (APTs), criminal enterprises, state-sponsored hackers and hacktivists as growing, and the top challenge to IT security.[4]

They're not wrong. In the UK, the government puts the economic cost of cyber crime at £27bn, a figure that is "significant and likely to be growing", with the loss to businesses comprising £21bn.[5] In Ponemon's 2016 State of the Endpoint Report, 78% of business reported an increase in the severity of malware attacks, up from 47% in 2011.

But the focus on external threats is somewhat misguided, and can lead to a quixotic concentration of resources in prevent and protect perimeter defence.

Although external attacks – viruses, malware, phishing – are more prevalent, insider attacks are costlier.[6] And many of those external attacks come from internal vulnerabilities; negligent employees ignoring security protocols, unsecured devices connecting to the network – something 81% of respondents to the Ponemon survey identified as the greatest threat to IT security.

This will only become truer with time. The endpoint is the weakest node in any network, and with the increase in BYOD, remote working and Internet of Things, the endpoints are multiplying. That means the number of entrances for hackers is multiplying too.

Far from the erstwhile controlled network of desktop PCs tethered by Ethernet, business networks have become amorphous, a tangle of devices both business and personal, accessing data through multiple WiFi nodes both onsite and off.

The situation is not unassailable. It simply means adopting a fresh approach to cyber security. New strategies that respond to the changing face of cyber crime. New technology that is capable of deflecting increasing sophistication from a growing threat.

In this white paper, we will examine the nature and scale of the threat – in order to better know our enemy – before tackling the question of how we tackle cyber security in the age of multiple devices, unsecured networks and the cloud.

[1] HPI Printer Security Research 2016 (Spiceworks)
[2] PAC Incident Response Management 2015: https://www.pac-online.com/download/19443/155514
[3] Ponemon 2016 State of the Endpoint Report
[4] IBM CISO Assessment 2014
[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[6] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic

The scale of the threat

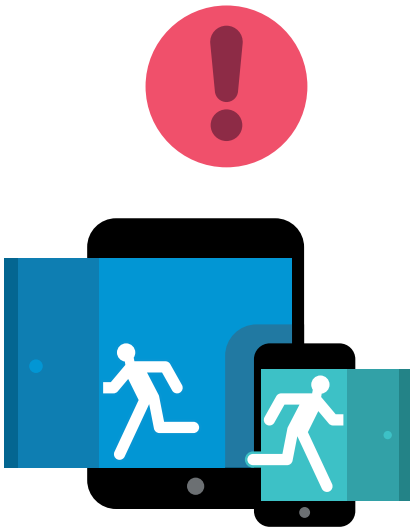
The average information breach costs companies $907,053 to recover from, with a further 13% loss in revenue. On average, it would take an organisation nine weeks to recover.[7]

Approximately 85% of companies surveyed in the HP Printer Security Report 2015 said they had experienced a security threat/breach within the preceding 12 months. 80% of IT professionals surveyed expected the threat to increase in the next three years.[8]

Cyber crime costs real money. Lost value from what is stolen or damaged. Lost revenue from reputational damage and lost productivity. Lost resources spent on recovery – support desk time, implementation of new security policies, staff losses and other internal responses. Fines and penalties from regulatory bodies. A decline in stock price.

The threat is only going to grow along with the number of devices connected to the network. Thanks to the Internet of Things, Gartner predicts there will be 11.4 billion connected devices by 2018, up from 6.4 billion in 2016. By 2020, more than 25% of identified attacks in enterprises will be IoT related, but IoT will comprise less than 10% of security budgets.[9]

The threat from cyber crime is big, and it's getting bigger.



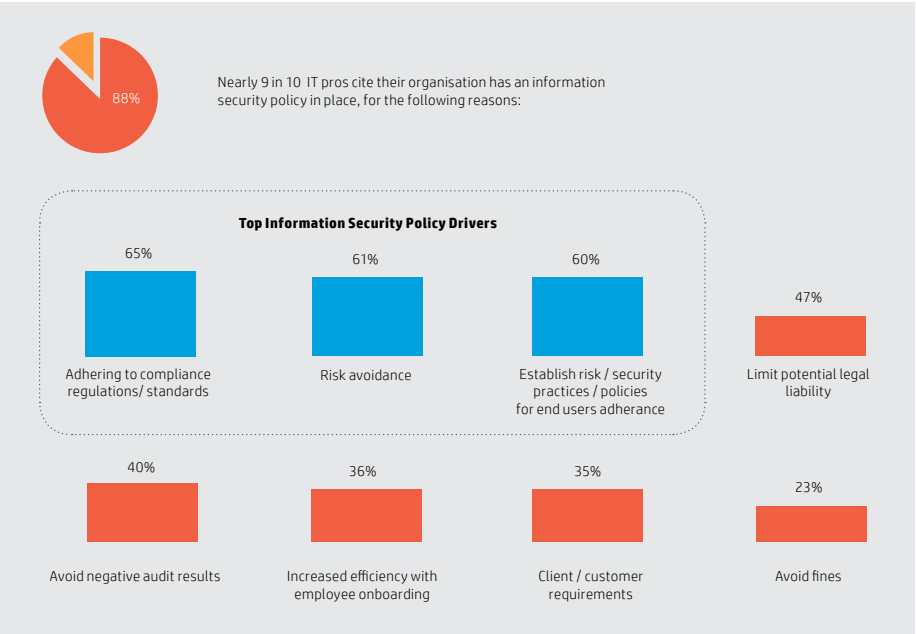
The form of the threat

Businesses are assailed by countless cyber attacks every day. Most are low level virus and malware attacks. 99% of organisations surveyed by Ponemon in 2016 had experienced malware in the preceding 12 months. External web-based attacks like these are relatively benign, costing organisations an average of $4,639.[10]

But more serious attacks are increasingly common. 51% of organisations surveyed in 2015 had experienced Direct Denial of Service (DDoS) attacks, which can be crippling – costing an average of $127,000. Even more alarming is that 35% had experienced a malicious insider attack, at an average cost of $145,000.[9]

The emerging picture is of relentless minor attacks from outside, with infrequent, but startlingly probable major attacks; which are probably enabled by insider negligence, if not maliciousness. 62% of organisations had experienced phishing/social engineering attacks, exploiting employee weakness for an average cost of $86,000.[11]

A separate survey by Spiceworks – on behalf of HP – broke down attacks experienced in 2014-2015 by 90 UK organisations.[12]



[7] NTT Security Risk:Value Report 2016
[8] HP 2Printer Security Report 2015
[9] http://www.gartner.com/newsroom/id/3291817
[10] https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-8392enw.pdf
[11] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic
[12] HPI Printer Security Research, Spiceworks 2016

How breaches occur

The headlines portray enterprising hackers besting sophisticated secure networks of governments and enterprises, but the reality is usually more sober.

Viruses may take advantage of compromised networks, but malware usually requires some form of user error. Phishing/social engineering attacks depend on them. Large DDoS and information theft attacks are often the result of user negligence as well.

The by now infamous Dropbox hack was reputedly the result of a careless Dropbox employee who used the same password for internal systems as for his LinkedIn account.[13] The alleged Russian hacking of the DNC was apparently thanks to John Podesta, former adviser to Mrs. Clinton, clicking a link in a phishing email mistakenly flagged as 'legitimate' by an aide.[14]

Hackers don't need active assistance to be successful. Just as dangerous is the ignorance of, or disregard for, security protocols. An increasing threat is employees bringing their own devices to work, using commercial cloud software, both of which introduce unsecured elements to an otherwise secure network; out of the control of enterprise IT, creating an unaccounted for vulnerability.

Most of the time, hackers needn't employ sophisticated algorithms or cutting edge technology, they simply need one of us to be a little careless.

The firewall is broken

The cornerstone of cyber security has until recently been antivirus and firewall software. Prevent and protect. Creating a secure perimeter. In the current working environment, that's simply not a credible strategy.

81% of Ponemon respondents say mobile devices on their network have been a target of malware. Other increases to security risks include employee use of commercial cloud applications – cited by 72% of respondents – BYOD (69%) and employees operating from home offices and offsite locations (62%).[15]

Put simply, a firewall made sense when, as network administrator, you could control which devices were connected. But in an era where employees are bringing their own devices to work – often multiple, often without the knowledge of IT – and increasing numbers of workers are connecting remotely, you simply can't protect the perimeter. Each unvetted device is a vulnerable endpoint for hackers to exploit.

[13] https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach

[14] https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0

[15] Ponemon 2016 State of the Endpoint Report

The HP perspective: moving beyond network security

Michael Howard, HP's worldwide security practice manager, on ensuring endpoint security

A key and current concern is that businesses are struggling to secure every endpoint due to a lack of awareness and knowledge about certain devices and the risks they carry. They feel safe behind a firewall, despite this being no longer enough to protect against an attack. Security teams must know every endpoint within the infrastructure and ensure that each endpoint has multiple layers of protection to guard against increasingly sophisticated attacks.

It's essential for security teams to investigate every corner of their business IT infrastructure and build an extra layer of protection on top of standard network perimeters. Firewalls alone cannot withstand sophisticated attacks and a defence policy with multiple protection layers on every endpoint is a must-have to ensure your business can meet regulatory requirements and avoid costly fines.

HP's policy is with every new solution, service or product that they develop security will be the first thing they look at. The development teams know that they have to answer the security questions and they have to know how they're going to put those on the network in a secure way.

More so than ever before, security should be a first, not a bolt-on. It's been HP's policy for years.

Layered security

A new approach to cyber security has to be multi-layered.
Network security is still important, but that must be formed of discrete networks itself. Many breaches rest on an initial entry that grants access to everything in the system. Think of John Podesta's phishing misstep. Ring-fencing sensitive information into multiple access tiers, so that stealing one key isn't conquering the castle, is essential.

Devices must be accounted for. A key issue for IT managers is ensuring each device connected to the network is protected by regularly updated security software – against viruses, malware and spyware – and are regularly scanned for anomalies. Better is to use the devices themselves as sensors, gathering real-time information to alert of any breaches to the network perimeter of which they are a part.

Comprehensive security governance must be in place, with every employee trained in cyber security protocols. Human error – from clicking the wrong link to connecting with a consumer device – is the number one threat to the network. Human error can be reduced with training.

Device security

Perhaps the largest issue confronting contemporary cyber security is control over which devices have access to the network.
The first, simple, solution often adopted is to have separate WiFi networks for guests and employees, so that unsecured external devices don't have access to the main network. This goes hand-in-hand with training employees to use this network with their personal devices.

The second is ensuring you have control over employee devices. This concern needs to feed in to the company's policy on BYOD or CYOD, and is a strong argument in favour of CYOD – which gives more control over which devices are used, choosing those that have better security features, how they are configured, and the management and monitoring of those devices.

Using one of our HP Elite range PCs, for example, is preferable to a budget laptop. Each HP Elite PC has HP SureStart technology that checks the BIOS every 15 minutes and resets the machine to its original state on detection of an anomaly, blocking unwanted intruders. For this feature – and many more – computers from our HP Elite 800 series were recently declared "the most secure PCs in the world."[16] But employees are unlikely to own an HP Elite PC themselves.

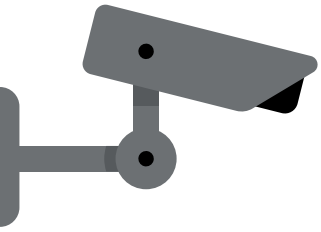
Employees often prefer to use their own devices for two reasons:
1. Consumer technology is often better than that provided by work
2. Employees like to use technology they are familiar with

By offering a well resourced CYOD policy, which offers the latest devices on a regular update cycle, organisations can provide better devices than employees' own, and maintain greater control over the security of those devices. This is what we sell our HP Device as a Service (DaaS) on.

It is essential to include all devices in the security strategy, even those often forgotten. In an IDC survey, 80% of respondents said IT security is important to their business, but only 59% recognised print security as important, although more than half had experienced a security breach involving print security in the preceding 12 months. This is an obvious blind spot.

The average number of security breaches before implementing a print security policy was 9.9 per year at an average cost of $521,400 (including fines). Following implementation of print security, the average number of breaches dropped to 1.5, saving 200 hours of employee time per year and $250,000 in related costs, including audit and compliance.[17]

[16] http://www8.hp.com/us/en/campaign/computersecurity/
[17] IDC The Business Value of Printer Security 2015



Proactive detect and response

77% of IT security spend goes on prevent and protect technology like antivirus software and firewalls, according to research by PAC. But this approach is ineffective. The research also found that 67% of firms surveyed had had a cyber breach in the preceding 12 months, and 100% at some point in the past.[18]

Antivirus software in particular is shockingly ineffective. Damballa conducted testing where they deliberately attacked a network to measure antivirus response. It took over six months before 100% of malicious files were identified.[19] This tallies with another PAC finding that it took between one and six months for firms to discover they had been attacked.

Keeping endpoints secure can no longer rely on prevention. The growing number of virus/malware incidents, plus the inherent insecurity of BYOD/mobile working means breaches are inevitable. No one is suggesting prevent and protect is abandoned entirely, but clearly detect and respond needs to climb higher on the agenda.

Continuous, real-time monitoring is necessary, ideally using endpoints themselves as sensors – alerting the rest of the network when they've been breached. This allows remote responses by IT security including processes such as:

- Remotely shutting down a device
- Killing an infected process, or one that's spreading malware
- Quarantining a specific file or group of files
- Disrupting network communications to isolate infected devices[20]

Accepting that breaches are bound to happen, and putting proper response protocols in place – as well as implementing the technology necessary to carry them out – is the only way to ensure cyber security when prevention can no longer be relied upon.

"No technology can deliver security if people undermine it."

– Joseph Steinberg [21]

Employee security

Just as important, if not more important than securing the device itself, is securing the person using it.
Every employee must be trained in cyber security. They must be aware of the risks of phishing. Of surfing suspicious websites. Of downloading suspicious attachments. They must be aware of secure password policy – using strong, unique passwords for every sensitive log-in, and using the right password manager to store them.

They must be made aware of the importance of keeping the security software on their device regularly updated, to ease the burden on IT's monitoring. They must be vigilant about using only secure devices to access the organisation's networks and avoid using personal devices on external, unsecure networks to access sensitive data.

Many high level cyber security experts recommend running simulated phishing attacks – going as far as building fake phishing websites to drill every employee – and taking cyber security training to a formal level. Because most attacks rely on exploiting human weakness, whether through negligence or maliciousness.

Because people are the weakest link in any network.

[18] PAC Incident Response Management 2015
[19] https://www.damballa.com/time-to-fix-malware-strategies-2/
[20] The Essential Endpoint Detection Checklist – HP Now
[21] https://digitalguardian.com/blog/data-security-experts-answer-what-biggest-misconception-companies-have-about-endpoint-security

Conclusion

IT security spend should shift from prevent and protect to endpoint detect and response

Defending an organisation's data in the current IT climate – faced with a mounting cyber crime threat and a loss of control over the network perimeter – requires two things: a conceptual leap and greater resources.

The concept of a network needs to change. The idea of the network as a fence around a collection of devices doesn't apply anymore. It's time to recognise the reality. 'The network' is a chimera. It emerges from connected devices – each an endpoint. Securing the network means securing the endpoint. And each endpoint consists of two elements: the device and the person using it. Both must be considered.

But enforcing security in this new paradigm is far more complicated than the simple desktop-PCs-connected-by-Ethernet environment of yesteryear. It requires greater resources, and these must be pushed for. Something that 61% of Ponemon respondents recognise.

The trick is getting the rest of the organisation on board. Only 36% of respondents felt they have ample budget and staff for endpoint security. 69% say the IT department cannot keep up with employee demand for greater support. 71% say endpoint security policies are difficult to enforce.[22]

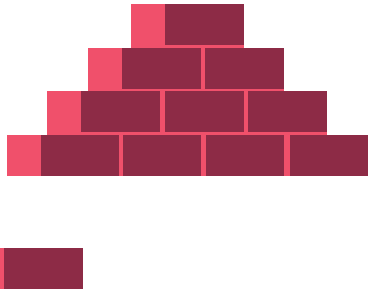
80% of IT security managers consider regulatory compliance the best way to justify funding their security programs, but also consider compliance the least important reason to spend. Compliance means meeting the bare minimum.[23]

IT decision makers must liaise with C-suite executives to underline the importance of security. Make clear the costs of lax security – the expenses of recovery, the lost revenue, the depleted share value – and impress the long-term savings. Many security solutions engender improvements elsewhere as well. Think of the improved productivity of implementing print security and the productivity benefits of providing regularly refreshed tech in a flexible CYOD program provided by third-party on subscription (like HP DaaS). A clear business case can be constructed.

The challenge is formidable. And with time – with the explosion of devices in the IoT era, and the increasing sophistication of cyber crime – it will only become more daunting. But it is not insurmountable. With the right tech, the right strategy and the right resources we can defend our endpoints. We can keep our data safe.

For more information and practical advice from HP's experts, download our **cyber security eguide.**

To find out more about HP Device as a Service, and how it can help you run a comprehensive, flexible and secure CYOD programme visit us **here.**



Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA7-1089EEE

[22] Ponemon 2016 State of the Endpoint Report

[23] https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697