Brought to you by

Contents

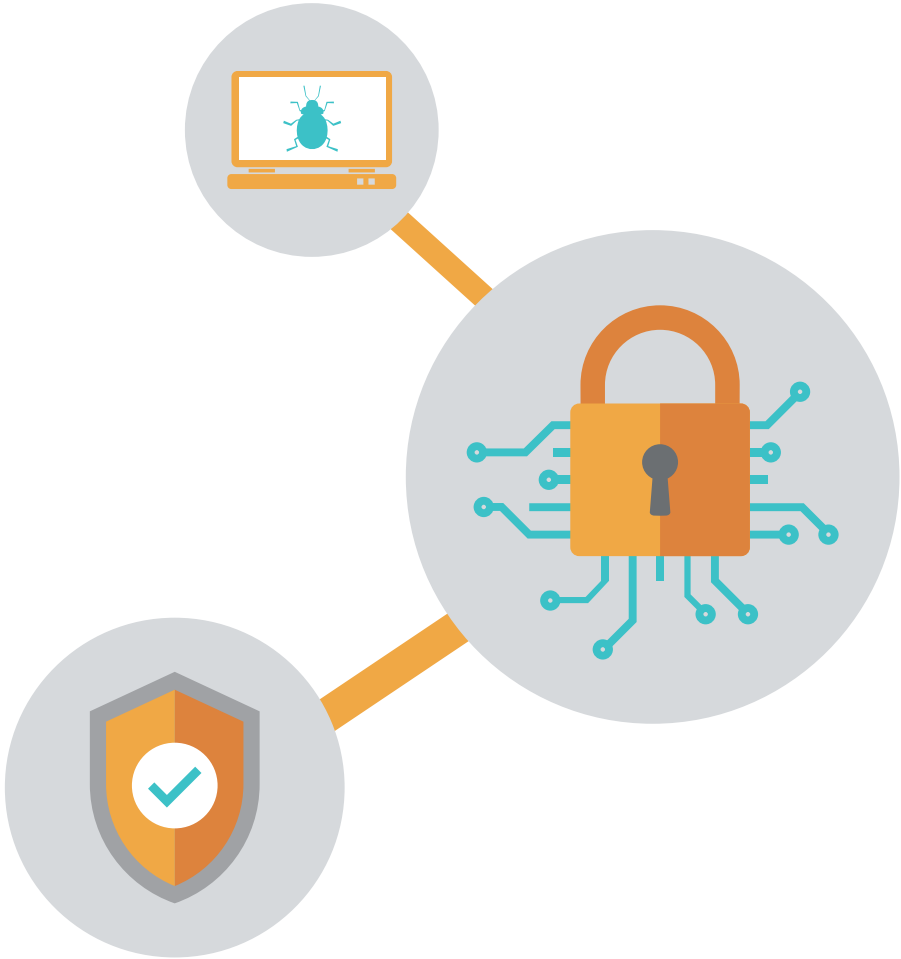
Introduction

"Many executives are declaring cyber as the risk that will define our generation." – Dennis Chesley, Global Risk Consulting Leading, PwC[1]

Cyber security is not a new threat. But it is a growing one. Hackers are getting better. And they have more points at which to breach a network. The Internet of Things is multiplying the number of endpoint devices, often the easiest entry point. Targets are increasing in size and disruption is increasing at scale.

On October 21st 2016, the US-based DNS provider Dyn suffered the largest distributed denial-of-service (DDoS) attack in history. Some of the world's largest websites – including Netflix,[2] Amazon and Twitter – were forced offline for hours.

In January 2017, Lloyds Bank suffered significant online outages. Customers couldn't check their account balances or make payments. Mobile app-based access was also down. Lloyds has not confirmed anything, but a DDoS attack was strongly rumoured to be the cause.[3]



Sources: [1] PwC: The Global State of Information Security Survey 2016 [2] http://thehackernews.com/2016/10/dyn-dns-ddos.html [3] https://www.theguardian.com/business/2017/jan/23/lloyds-bank-accounts-targeted-cybercrime-attack

Introduction

Breaches like these are more than bad publicity. They cost real money.

In the 2016 Printer Security Survey Report from Spiceworks, 34 percent of organisations said a breach meant increased help desk calls/ support time, 29 percent said breaches reduced productivity/ efficiency, and 26 percent reported increased system downtime as an issue.[4]

Close to 60 percent of security leaders interviewed for an IBM CSO Assessment paper said the sophistication of attackers was outstripping the sophistication of their organisation's defences.[5]

Worried CIOs have cited cyber security as a top 10 issue for over a decade, now it's number two in the annual SIM Trends study.[6]

A lot of this damage is preventable. In the following pages we will cover common misconceptions about cyber security, take a more detailed look at the impact cyber crime has on businesses, and what you can do to better defend against attacks. Finally, we'll peer into the future and discuss what's to come, and how to prepare.

Sources: [4] HP Printer Security Research 2016, Spiceworks [5] IBM CSO Assessment 2014 [6] SIM IT Trends Survey 2015

Cyber security myths debunked

Five Common Misconceptions
that can put businesses at risk of cyber crime

Household names may make the headlines for data breaches, but all types of organisations are at risk. Here are five myths about cyber security that can leave businesses vulnerable to hackers.

Security Breach

Security Leaks

Security Practices

Antivirus Software

Cyber Attack

1 Businesses can recover quickly from any breach

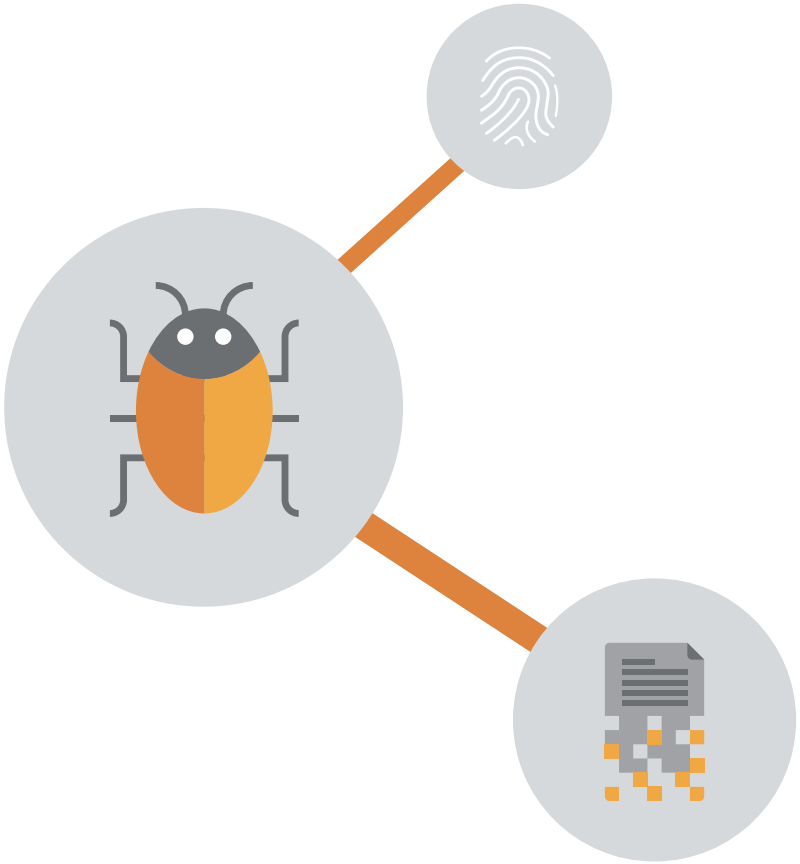
It's still very difficult to measure the cost of cyber security breaches to commercial organisations. The belief used to be that you could see the impact of any breach through declining stock prices.

But stock prices are only part of the story – and the first part at that. While stocks may recover within a few weeks, longer term costs accumulate. New security programmes. Replacement personnel. Legal expenses.

All these factors can significantly disrupt a business for long periods of time following a breach. And the costs are going up. A recent Ponemon study found the mean annualised cost of a breach increased from **$7.7million** in 2015 to **$9.5million** in 2016.[7]

Source: [7] Ponemon Institute Cost of Cyber Crime Study 2016

2 Security leaks happen rarely, so serious protection isn't needed



The IDC found[8] that the proportion of businesses experiencing a breach reached 99 percent in 2016. While the number of companies reporting being breached 6-10 times in a year leapt from 9 percent in 2014 to 18.9 percent in 2016.[9]

These figures may well be on the low side. Breaches are often significantly under reported as companies seek to avoid the negative press that goes with them.

The other point this myth misses is the debilitating impact a leak can have. Maybe your company does only suffer one leak. But one leak could cause significant challenges.

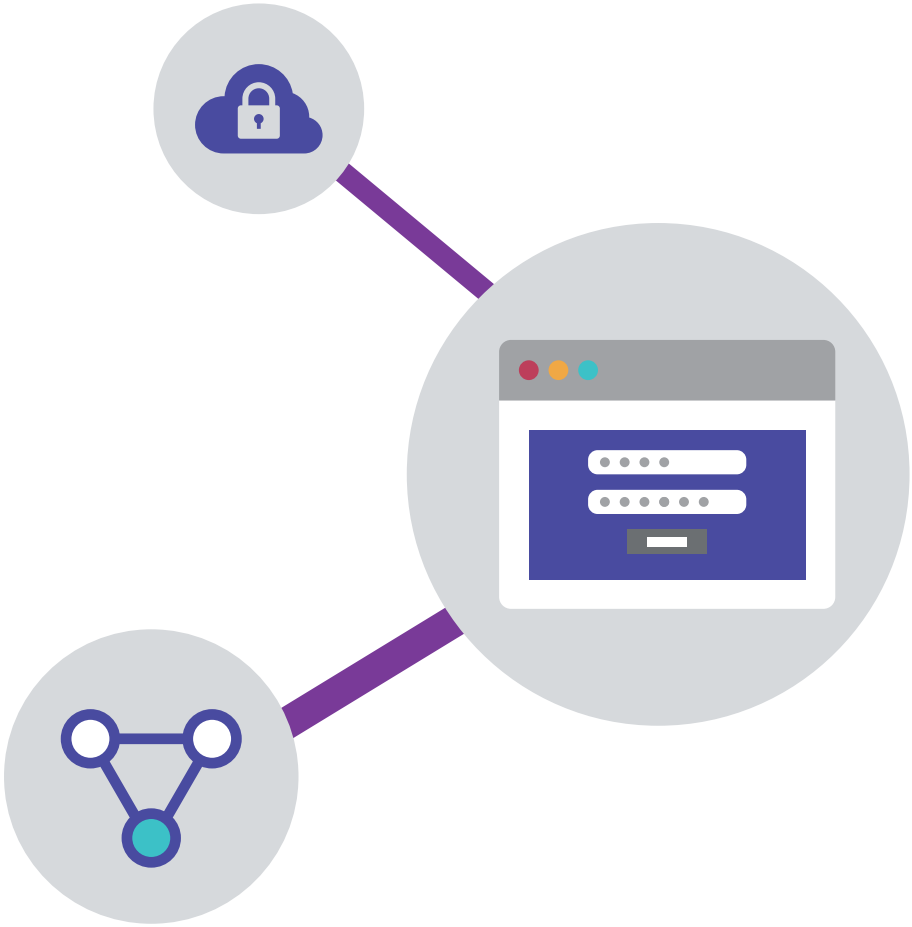
Sources: [8] IDC [9] Ponemon Institute Cost of Cyber Crime Study 2016

3 We've hired an IT specialist to handle security, so we don't need to know anything else

While hiring an expert is a good idea, every employee in the company should also be trained in good cyber security practices.

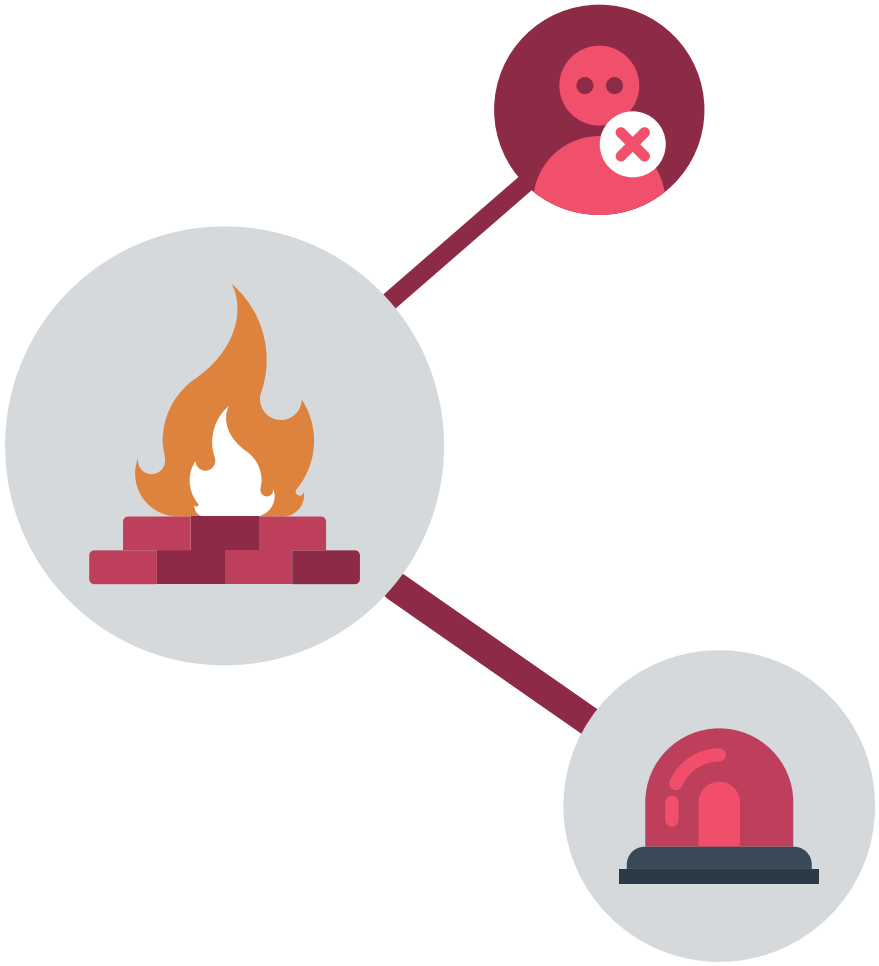
Think of the colleague who unsuspectingly downloads a malicious email attachment or visits an unsafe website, infecting a company network with malware that slows down computers or sends sensitive information to a cyber criminal.

According to the 2016 Cyber Threat Report by CyberEdge, organisations ranked 'low security awareness among employees' as the leading issue that inhibited them from defending themselves against security threats. This ranked higher than 'lack of budget' and 'lack of skilled personnel'.[10]



Source: [10] Ponemon Institute Cost of Cyber Crime Study 2016

4 We have strong antivirus software on our systems, so we're well protected



Antivirus software works by scanning systems for malware downloaded from websites or emails. But attackers have other means to bypass this protection.

Cyber attacks that cannot be blocked by antivirus software include distributed denial of service attacks (DDoS), where a website is flooded with junk traffic that slows it down or stops it working; web-based attacks, where hackers inject malicious code into a site for purposes such as data theft or remote spying; and hackers gaining access via stolen devices.

5 If an intruder gets in, we'll notice right away

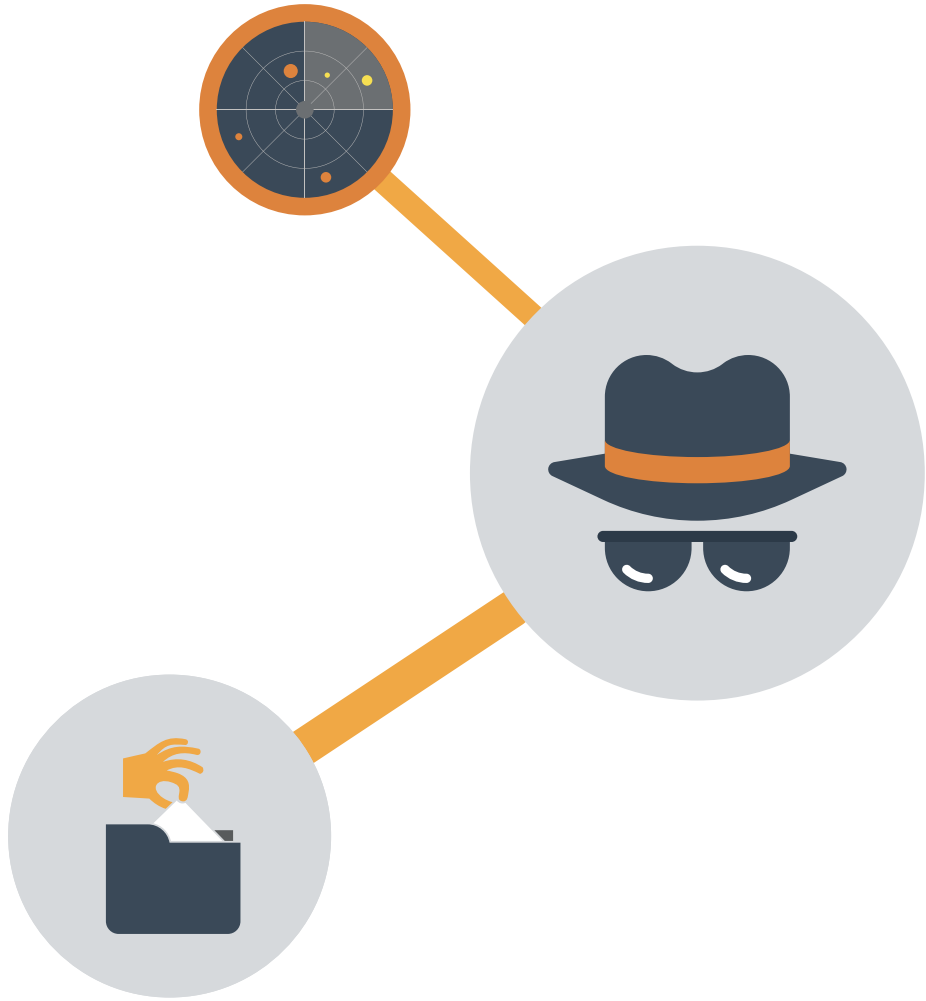
It isn't easy to detect a cyber attack. Malware that enters a system may not immediately disrupt operations; instead, it may spy on the system giving the hacker information to plot more targeted attacks, often to gain access across the network.

Such attacks on specific systems are categorised as advanced persistent threats (APT). APT attacks are characterised by continuously monitoring and obtaining data from a particular computing infrastructure over time – usually undetected.

IT consultancy Daisy Group estimated that half of UK businesses could be hacked in less than an hour.

TIP:
Monitoring outbound data for higher-than-usual traffic can help identify data theft – it may be an APT attack.

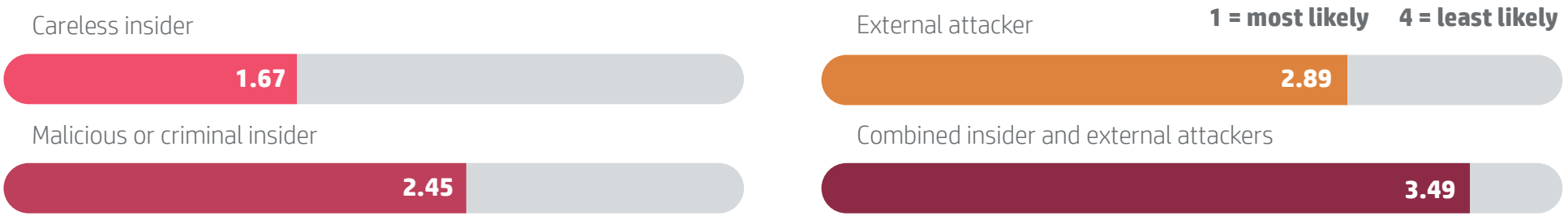
TAKE ACTION:
Choose security software with data protection, such as HP SureStart, which automatically restores a computer's BIOS when a malware attack is detected – stopping breaches before data is compromised.



Where do threats come from?

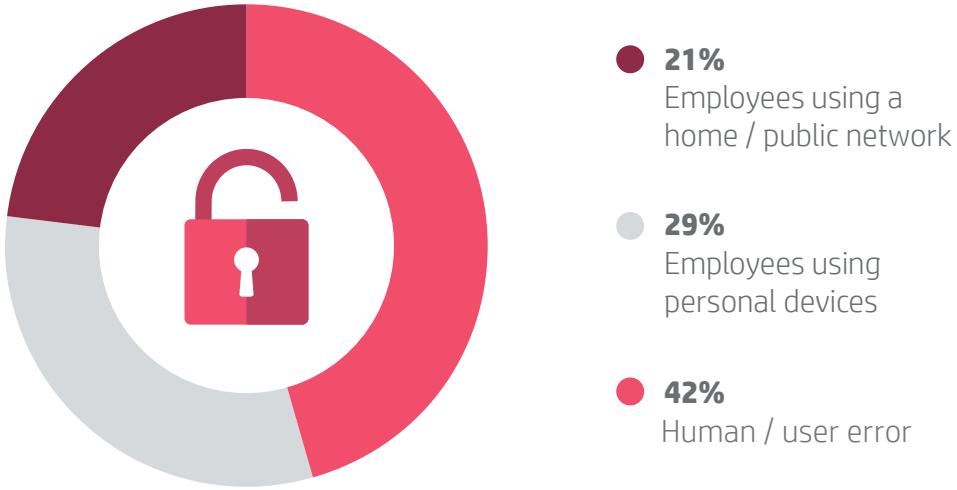
Protecting your network starts with knowing your weakest links

The most likely cause of data breach:[11]



Most common types of external threats:

How internal breaches occur:[12]



Sources: [11] http://www.kilpatricktownsend.com/_assets/Kilpatrick%20Townsend%20Report%20Final.pdf [12] Ponemon Institute Cost of Cyber Crime Study 2015

How much does it cost to recover from cyber crime?

The most costly types of cyber attacks:

25%

£1,000,000

Malicious code & malware

Software that harms a system by creating security holes, damaging files or stealing data (includes scripts, viruses and worms)

24%

£960,000

Distributed Denial of Service

"DDoS" attacks are floods of web traffic that take down a company's site and servers

16%

£640,000

Web-based attacks

Attacks targeting visitors to your site, such as injected code that redirects browsers to malware-loaded sites

13%

£520,000

Stolen devices

Lost employee devices with access to company logins can lead to data theft and identity fraud

9%

£360,000

Phishing and social engineering

Emails or pop-ups posing as legitimate requests for logins

9%

£360,000

Malicious insiders

Employees who give away sensitive information

4%

£160,000

Botnets

Networks of infected computers that are controlled for malicious activity such as sending spam

Source: [13] Ponemon Institute Cost of Cyber Crime Study 2015

The impact of cyber crime on businesses

The true cost of cyber crime extends beyond repairing the damage of a hack

Security breaches are incredibly costly. Broadly speaking, there are three ways that a breach could hit your company's finances.

Company Resources

Obviously you'll have to get things in order. This uses a significant amount of employee time and cost. Meaning you may have to put other, revenue-generating work, on hold.

Fines / penalties

You may be hit with a fine for noncompliance (e.g. HIPAA). Once EU GDPR comes in next year, companies found negligent could incur a total fine of 4% of their global turnover. You may even be at risk of lawsuits if the leak results in a breach of client-customer confidentiality.

Damaged reputation

This can be one of the most damaging impacts of a breach. Customers, the press and the public at large have a long memory for security breaches. It can take a long time to recover trust.

Anatomy of the unexpected hack

When Sony Pictures was hacked in 2014, the hackers simply walked in the front door.[14]

According to "Lena" of hacking group Guardians of Peace (GOP) – who claim responsibility for the attack – Sony "don't do physical security anymore." They gained access to Sony's network by physically entering the building and stealing the computer credentials of a system administrator.

Once in, they planted malware that grabbed private files, source code and passwords for Oracle and SQL databases. From there, they stole movie production schedules, emails, financial documents and more – and published much of it online.

The hackers threatened to publish further secret and top secret data if the company didn't pull the film "The Interview" from cinemas.

Sony eventually capitulated, losing untold box office receipts, as well as incurring incredible reputational damage.

Sony made two mistakes. Not accounting for physical access to company data by intruders, and not investing in multiple layers of security - which could have prevented access to sensitive information following the initial breach.

As security expert Bruce Schneier wrote after the attack, "Against a sufficiently skilled, funded and motivated attacker, all networks are vulnerable." The trick is recognising where your network is vulnerable. It may be the front door.

TAKE ACTION:
Create a breach response plan for every department from IT to customer service to minimise recovery time.

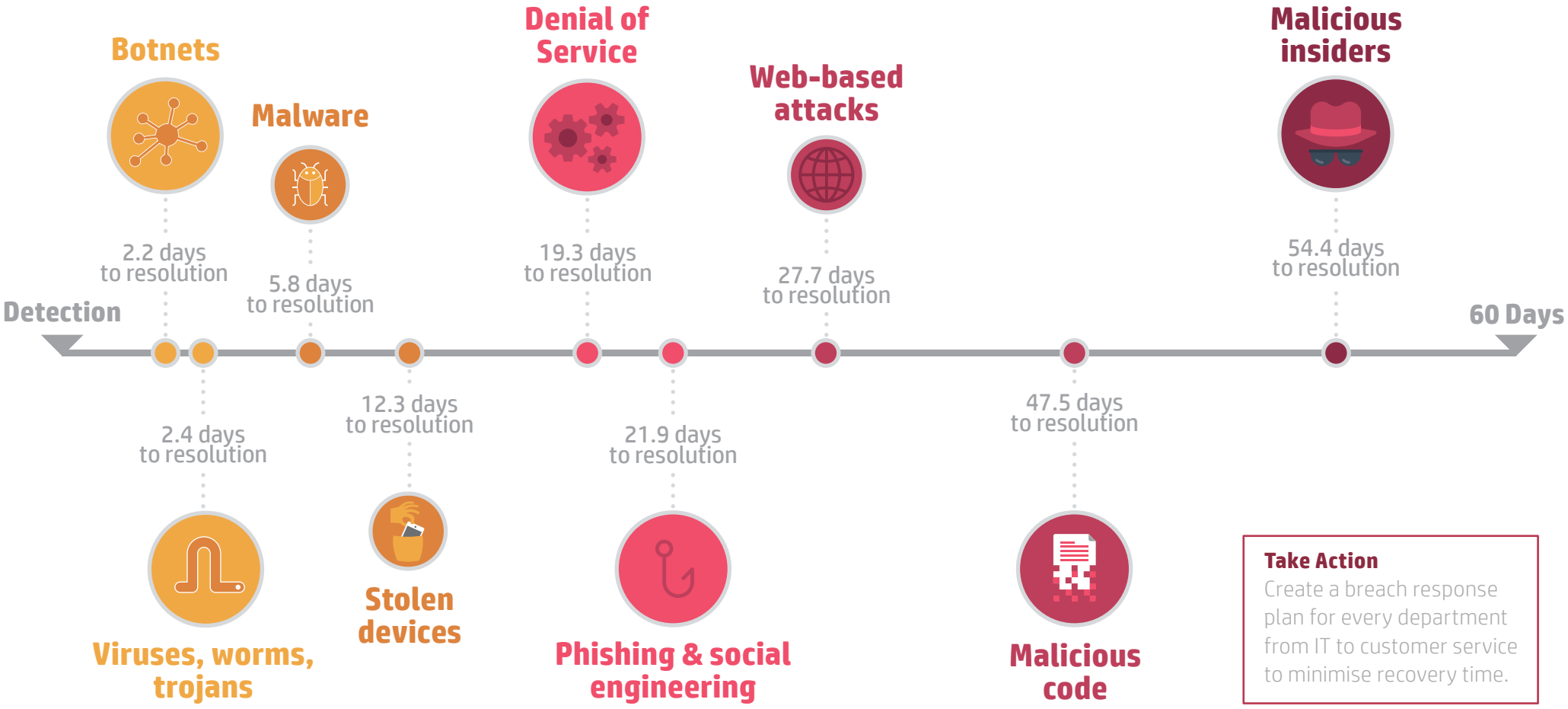
TIP:
Many forms of malware are passed on as email attachments. Train staff in recognising suspicious files designed to look like legitimate documents.

- Estimated cost of cyber crime to UK businesses: $21bn[15]
- Average cost of cyber crime per UK company in 2016: £5.7m[16]
- UK enterprises that experienced a cyber breach or attack 2015-2016: 66%[17]

Sources: [14] http://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12?IR=T [15] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[16] https://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/ Stat is $7.21m – have converted to £
[17] https://www.gov.uk/government/news/two-thirds-of-large-uk-businesses-hit-by-cyber-breach-or-attack-in-past-year

Cyber crime: the recovery time

How long does it take to repair the damage of a data breach? The Ponemon Institute[18] puts the average at 46 days, a potentially crippling figure for UK SMEs banking on operating without interruption



Take Action
Create a breach response plan for every department from IT to customer service to minimise recovery time.

Source: [18] Ponemon Institute Cost of Cyber Crime Study 2015

How to protect your business from cyber crime

Essential tips and strategies for business cyber security

Here are six common targets for hackers breaching company systems and what you can do about them today.

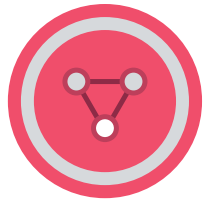
Customer Databases

Cloud Services

Staff Smartphones & Tablets

Employee Errors

Internet of Things



Network Gateways

As we shift to an increasingly digital world where more value than ever is placed on data, cyber crime can take many forms. Cyber criminals are often after information, and with more connected devices used in the workplace – from smartphones and tablets to WiFi printers – there are a growing number of access points for hackers to target.

1 Customer databases

Financial data is far from the only target for attackers – information such as names and email addresses can be used for identity fraud, spamming, or to hack other accounts.

A major prize for serious hackers is cracking businesses that serve even larger businesses. Think of it as the digital equivalent of breaking into a hardware store just to get access to the basement wall shared with the vault room of a neighbouring national bank.

Once attackers are inside the smaller system, they are better placed to gain access to the customer data held by its large company clients. How might your customer database be compromised? Viruses, worms and trojan horses – downloaded from malicious sites or emails – can unleash the necessary code for a hacker to enter and steal data.

How to protect your customers' data

- Use security software designed for businesses, which offers network, email and endpoint protection.
- Always update your security software to block evolving malware.
- Download software updates for your system programs, as older programs can contain vulnerabilities for attackers to exploit.

2 Cloud services

How to protect your customers' data

- Encrypt your most important information using tools such as PKWARE's Smartcrypt technology, which uses access policies to determine the complexity of encryption. That way, authorised users see the data they're supposed to see – and unauthorised users see nothing.
- Create a strong password for your cloud account. Also, in the settings for your cloud account, define precisely who can access your data and what they can do with it.
- Require two-factor authentication - such as a smartphone code as well as password – to make changes to cloud data, such as downloading, deleting, or moving files.

Cloud computing has become a staple of enterprise infrastructure.

The 2016 IDG Cloud Computing Survey[19] found 70 percent of enterprises have at least some infrastructure in the cloud, while Tripwire found that 90 percent use the cloud for infrastructure and/or data storage – including mission critical data.[20]

Security is of course a concern, but in reality data is usually more secure in the cloud – stored on off-premise servers by a company whose reputation is staked on keeping it safe.

That's why 64 percent of enterprises surveyed by Tripwire view the cloud to be more secure than legacy systems.

Happily, this trust isn't misplaced – according to the 2015 BIS survey,[21] just 7 percent of businesses (large and small) suffered a serious breach of their cloud services, and these are generally as a result of access permissions or insufficient passwords. However a secure cloud still needs robust internal security governance. Just think about Sony's front door.

Sources:
[19] https://www.scribd.com/document/329518100/IDG-Enterprise-2016-Cloud-Computing-Survey
[20] https://www.tripwire.com/state-of-security/security-data-protection/enterprise-impressions-of-cloud-security-in-2016/
[21] 2015 Small Business Survey. Department for Business, Innovation & Skills

3 Staff smartphones and tablets

Many people use their personal devices for office tasks.

Bring-Your-Own-Device (BYOD) policies for businesses are an effective way to leverage smartphones that employees already own. This trend is increasing, with 53.2 percent of organisations implementing a BYOD policy within the next two years.[22] But these devices can be a ripe target for hackers.

An estimated one in five Android apps carry some form of invasive malware, which could be passed on to company files and systems to monitor activity or steal information.

This threat is increasing, with 64.9 percent of organisations saying the volume of threats targeting their mobile devices has increased.[23]

Employees who have their phones stolen can also unwittingly be the doorway for hackers. A phone thief may sell a device to a black market buyer, who can pick it apart for information to breach the victim's company, or penetrate the systems of a larger client. Organisations rated their ability to defend security threats originating from mobile devices at 3.54 out of five. This was the lowest rating for all the potential origin of threats they were asked about.[24]

How to secure staff-owned devices

- Install a threat-detection tool such as Duo's X-Ray for Android devices to make it easier to track rogue apps and suspicious code.
- Ask employees to enable remote-wipe (available free for Android, iPhone and Windows Phone; with subscription for BlackBerry) so that in the event of loss, sensitive data both business and personal can be erased.
- Ask employees to enable device encryption on their smartphones to protect data (this is on by default on new iOS and Android phones).

Source: [22] 2016 Cyberthreat Defense Report, CyberEdge [23] ibid [24] ibid

4 Employee errors

How to help your staff

- Educate your staff in cyber security best practices and provide regular training to stay abreast of the latest threats.
- Develop a security protocol tailored to your business and the types of data it processes.
- Create a team for communicating your cyber security policy to employees as well as clients and business partners.

The most basic tenet of cyber security is a good password policy, and yet, 31 percent of the worst security breaches in 2015 were the result of a staff-related incident.

From hacking weak passwords to stealing documents emailed over an unsecured connection, or a phishing email targeting a specific employee, attackers often exploit human error.

5 Prepare for the Internet of Things

Research firm IDC predicts the number of devices connected to the Internet will reach 30 billion in 2020, up from an estimated 13 billion.[25]

While office computers are secured at least by passwords and ideally by security software, print queues and print jobs are often not protected by similar security protocols.

Such unsecured printers – and other networked hardware – may fall prey to 'sniffing programs' that can log print jobs as well as network traffic, usernames and password information, all sent back to a cyber crime server.

It is worth noting here that the highly publicised Dyn breach was reportedly linked to a network of web-enabled CCTV cameras made by a single company, XiongMai Technologies. According to security firm Flashpoint.

This illustrates that every device on your network is an end point, and your network is only as strong as its least secure device. Some 97 percent of organisations have security practices for desktop/ laptops, 77 percent for mobile devices, and 57 percent have security practices in place for printers.[26] The only way to stay secure is for all businesses to have security practices for every endpoint device.

How to prepare for the internet of things

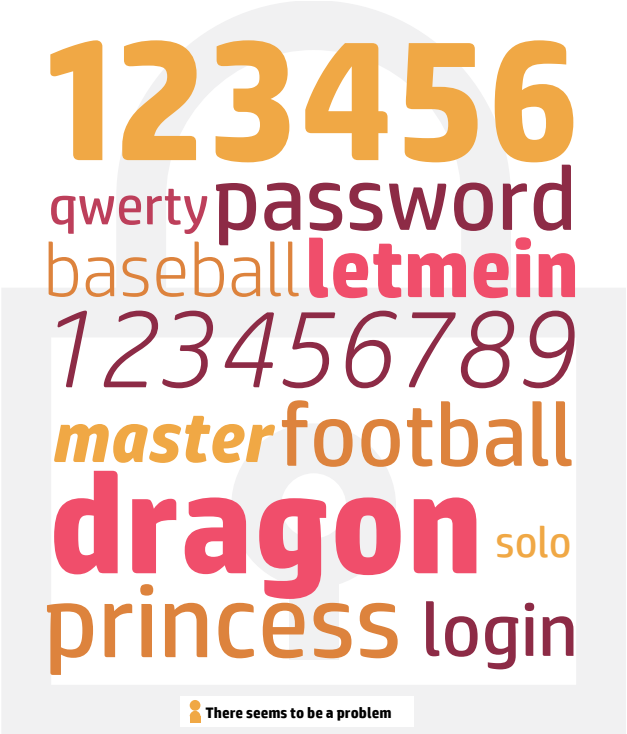
- Remove or disable unnecessary functionality on hardware since more functions can create more gateways for attackers to enter.

Sources: [25] PwC: The Global State of Information Security Survey 2016 [26] HPI Printer Security Research, Spiceworks 2016

Passwords and ransomware

The most common passwords

In early 2013, an Ars Technica reporter who had never been a cyber criminal nor had any experience breaking into password-protected systems cracked 8,000 of more than 16,000 encrypted passwords in one day*. So what chance do these extremely common passwords have against a determined cracker?



What is ransomware

Cyber criminals have increasingly turned to ransomware, a form of malware that hijacks systems that can then only be unlocked with delivery of a ransom in bitcoin. Thousands were affected in a 2013 outbreak of a trojan called Cryptolocker that caught the attention of the UK's National Crime Agency and its National Cyber Crime Unit. Here's a closer look at how these types of attacks work.

1. Installation	Malicious code works itself into your computer after an unintended download, through an email or malicious website.
2. Alerts its headquarters	Ransomware connects with its home server to establish an encryption key.
3. Encrypts your files	Ransomware scans the files on your network and encrypts them, rendering them inaccessible.
4. Extortion	A message usually pops up on the user's computer displaying a time limit and amount to pay up in order to decrypt the files before they're deleted.
5. Paying up	Business owner may purchase a digital currency like bitcoin to transfer to the attacker, who hopefully decrypts the files.

* Splashdata

6 Network gateways

When hackers want entry to a network, they may unleash a DDoS attack – thousands of machines infected with malware are united to generate so much junk traffic that the network falls under the weight of the attack.

Often, DDoS attackers want to distract site administrators with a frozen system while they steal data or install malware to plan future data heists. Some DDoS attacks are also the result of 'script kiddies,' novice hackers who simply want to take down a website because they can. Even a few hours of website downtime can be devastating for a business' bottom line and reputation.

TIP:
Invest in hardware that offers in built protection such as advanced authentication and tools for encryption.

How to secure your network

- Construct systems that check the traffic travelling in and out of your network. A sudden spike could indicate an attack, while constant but unexplainable activity could indicate that a trojan is reporting data back to its mothership.
- Filter all traffic so that only traffic required to support your business ends up on your network.
- Make sure every router, switch or other network device is operating with the same baseline software and functionality, and always download software updates.

The future of business cyber security

With businesses so internet-dependent, it is increasingly crucial to build solid cyber security defences.

Today, employees bring their own devices to work. Businesses employ cloud computing platforms and outsource key technical services. And more people now work remotely. Cyber security gets tougher when you control neither the device nor the infrastructure nor the workspace.

At the same time, smartphones have taught us that business can be done anywhere at any time. A café is just as good a place to work as an office. We use public WiFi networks to process vast amounts of business and personal data – often over smartphones that are weakly secured. Criminals certainly notice the shift. Security suffers when we don't heed the circumstances of our work.

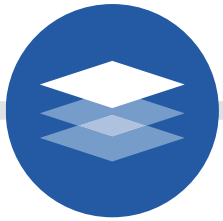
In the years ahead, that's going to mean much more than adding antivirus software to our devices or updating passwords every six months. Rather, businesses must embrace enhanced security measures that work just as well remotely as they do in an office governed by an IT administrator

For the distributed organisations of tomorrow, cyber security hinges on sophisticated analytics that isolate unusual behaviour, and layered security that protects all access points.

The future of business cyber security

Analytics: the cyber security detective

Even if your site doesn't get heavy traffic, it will have patterns. Using analytics tools that measure and log activity can make it easier to diagnose when something is wrong. These tools work by tracking and documenting normal behaviour first in order to detect anomalies later. Once detected, administrators can then go on the offensive and remove attacks before they get the chance to unleash cyber chaos.



Layering: keep attackers one step behind

Sometimes referred to as 'defence in depth,' layered security protects each access point in multiple ways. Common approaches include extended validation SSL certificates that make it difficult to fake the credentials required to enter a secure network. Backing that with multi-factor authentication that requires invaders to crack more than just a password can also be useful.

Regardless of the specific technology at work, the principle behind layering is to have every sensitive area of your business network locked down in some fashion. Your users and partners may need extra time and effort to access crucial data, but what you trade in inconvenience should more than pay off in peace of mind for your business.

Take action now

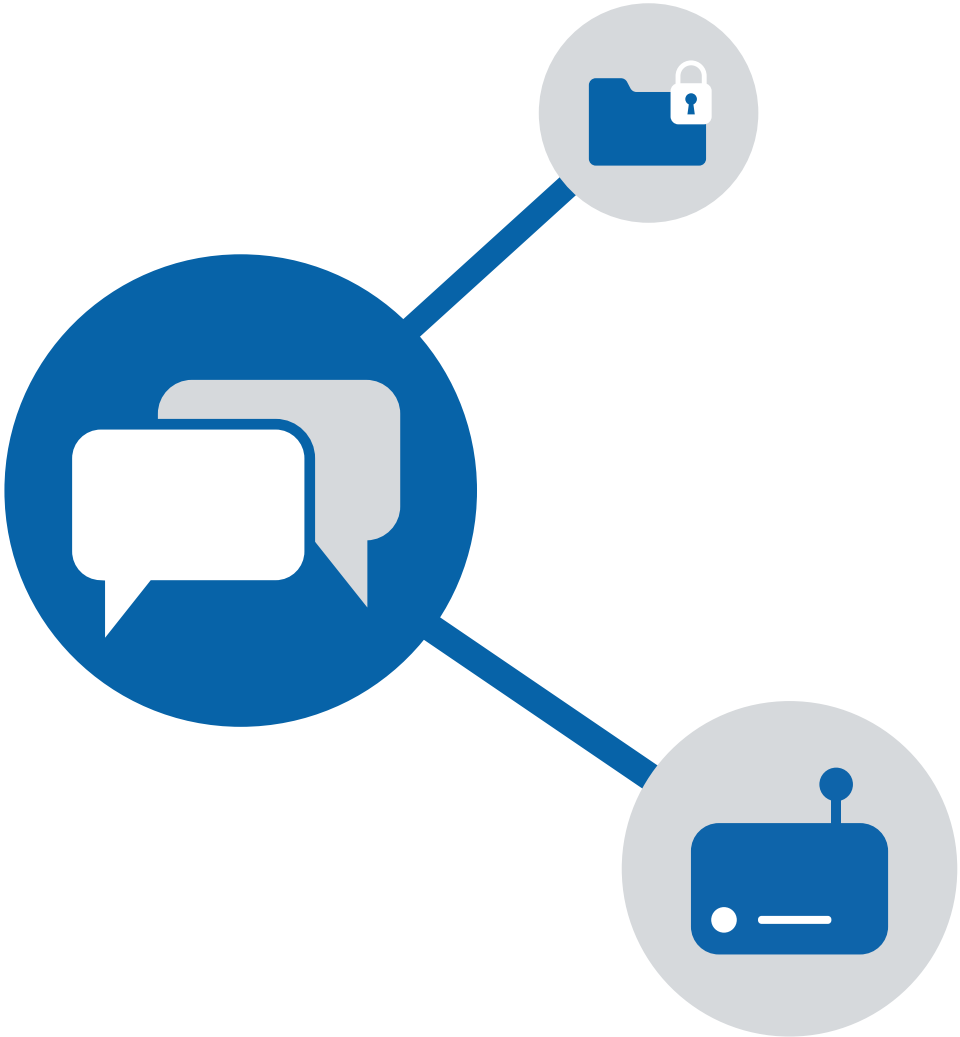
Investing in cyber security software and training is the best defence. Start by doing an audit of your systems and infrastructure. Are you doing enough? What could you do better?

Finally, you can also call our experts here at Hewlett Packard Inc. Our collective knowledge base is focused on staying ahead of threats, not just responding to them. To find out more, please visit us at HP.com.

TIP:
Track and document normal behaviour first in order to detect anomalies later.

Considerations for endpoint device security

Securing every single device on your network



Security research carried out by Spiceworks[27] found that the main source of security threats facing businesses were:

- Laptops and desktops: 81% external and 80% internal
- Mobile devices 36% external and 38% internal
- Printers 16% external and 16% internal

Which of these threats is in most urgent need of being secured? All of them, is the very simple answer. While this may be starkly obvious, an alarming number of organisations are still cherry picking which devices to secure.

The HP perspective is that any device that connects to your network must be secured. Put simply: your network is only as secure as your least secure device.

The intuitive logic may tell you that securing a connected printer is not as important as securing your fleet of laptops. But the risk is the same. Hackers are known to target things like printers, or any smart device that connects to your network. They know that these devices are typically not very well secured, yet they provide the same level of access to your network.

Source: [27] HP Printer Security Research 2016, Spiceworks

HP: Leading the way in a new landscape

Cyber security is changing. We have the tools to help your defence.

There are no quick fixes in cyber security. A robust defence requires a multi-faceted approach encompassing networks, devices and people. Choosing the right technology is a strong start.

At HP, safety comes first. The HP Premium Elite range of devices feature market-leading security features unavailable elsewhere, like HP SureStart – the world's first self-healing BIOS.

HP are equipping their devices with:

- **Bluetooth lock:** Using Bluetooth, the machine automatically locks when you walk away, and unlocks when you return.
- **Biometric security:** Facial and fingerprint recognition give access only to biometrically authenticated users.
- **HP SureView screens*:** The darkened monitor prevents onlookers from seeing your screen, protecting confidential material when working on the go.
- **HP SureStart self-healing BIOS:** Every HP Elite monitors its BIOS every 15 minutes. On detection of an anomaly it resets the PC to its original state, ejecting any intruders.

HP's Elite range won't protect your business by themselves. But they'll build a strong front line. Visit www8.hp.com to find out more about the complete HP Elite range.

* Selected models

Glossary and further reading

Access governance tools

Botnet:
Generally refers to a type of automated program designed to access and control Internet-connected computers without the owner's knowledge. The computers are often infected with malware. Hackers use botnets to unleash a **Denial of Service attack** on a website.

Data loss prevention tools:
A broad category of software whereby the goal is to monitor sensitive data and block attempts by unauthorised personnel to access or copy it. Different approaches allow for protection at the point of access (i.e. the endpoint), while traversing a network, or in a file system. Gartner had this market **growing by 25 percent** in 2013.

Encryption technologies:
Tools that **make the data itself unreadable** without some sort of decoder. The UK Information Commissioner has come out **strongly in favour** of various types of encryption in past years. More recently, the government has been forced to **reverse its position on encryption technology** in the wake of severe criticism.

Firewall technologies:
Another broad term that describes a style of device that uses algorithms and other techniques to block unauthorised traffic and users from entering a network. **Next-generation versions** of these devices can be potent for how they combine functions that had previously been handled by distinct devices. Intrusion detection, for example. They also tend to be application-aware, and thereby know the difference between web traffic from a salesforce.com implementation and from a Facebook page.

GRC tools:
Meant to refer to broad and coordinated initiatives inside a company aimed at managing and governing operations in a way that's compliant with regulations, and which, as a result, reduces risk.

Malware:
A broad category of software that can cause harm to or even disable other systems. Viruses, worms and trojans are all examples of malware. Also, for the purposes of the Ponemon study cited throughout this eBook, malware is considered distinct from viruses, which it says "reside on the endpoint and have not yet infiltrated a network".

Perimeter controls:
A general category describing cyber defence at the point where the public Internet or other public network meets a private and locally-owned and managed network. **Multiple layers and types of devices** are usually involved.

Phishing:
Usually conducted via email, whereby an attacker asks for identifying information in a legitimate-looking dialogue box.

Policy management tools:
Broadly speaking, policy management tools set a standard for what certain users can and can't see, and then enforce that policy across an entire network. Consistency (in theory, at least) ensures security.

Glossary and further reading

Security intelligence systems:
A wide variety of security intelligence can help gather and synthesise information relating to threats. Systems vary from log managers to systems for detecting network anomalies.

Social engineering:
Wherein an attacker works to coerce an authorised user to give up information they shouldn't, granting an attacker access.

Trojan horse:
Like a virus or worm in its impact, Trojan horses must be installed by the user, and as such, tend to be cleverly disguised. Effects can range from changing computer settings, to deleting files to creating a "backdoor" for a hacker to exploit later.

Viruses:
Malicious code that is capable of replicating and spreading across a network.

Web-based attacks:
Most often a web-based attack involves redirecting a browser to a malicious site.

Worms:
Unlike viruses that spread when a host file is shared, worms can replicate independently of a host file such as a Word document or Excel spreadsheet and therefore need no additional human interaction to wreak havoc. Instant messaging systems are well-known to have spread worms; Skype suffered that indignity in 2012.