Cyber Crime

The threat to small and medium sized businesses

HSBC

Cyber Crime: What does it mean for you?

Technology is at the core of our everyday lives, so much so that for many of us it's difficult to remember a time without mobile phones, computers, email and the internet.

These innovations have changed the way we connect with one another, both on a personal and business level. Technology has played a key role in how the world economy has evolved over the course of the last decade, but it's also given criminals new tools for gaining access to information and funds.

From malicious insiders to hackers and phishing schemes to malware, criminals are getting smarter and more innovative. A look at some of the most recent high profile security breaches reported in the news show how malware allowed cyber criminals to gain control over the computer systems of a large entertainment corporation while hackers were able to gain access to millions of a global eCommerce company's customer records.

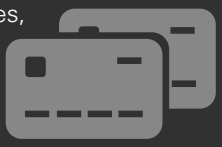
What might be surprising, however, is that in their most recent Internet Security Threat Report, Symantec found that 60% of all targeted attacks were levelled against small and medium-sized (SME) businesses. One reason for this is that SMEs could be perceived as somewhat more vulnerable with fewer resources to invest in security. Unfortunately, they may also have fewer resources to recover from an attack. A well-known code-hosting firm, for instance, was forced to shut its doors after a cyber attack that lasted all of 12 hours.

It's critical that you are up-to-speed on what criminals are doing and – more importantly – what you can do to minimise the likelihood of becoming the victim of these types of attacks. To that end, we also focus on educating our customers, which is why, in addition to online resources[1] we've developed this overview to give you a snapshot of the cyber crime landscape in general, as well as in terms of specific threats to small and medium sized businesses like yours. In the pages that follow you will find some examples of the most common types of cyber crime and how they might impact your business, combined with a synopsis of best practices for keeping your data and systems as safe as possible.

[1] *If digital, links to http://www.hsbc.com/internet-banking/online-security - if print, references URL in a footnote*

PERPETRATORS

Hackers: A Multinational eCommerce Company, February through May 2014 – The company's customer database was hacked sometime between late February and early March of 2014 – giving hackers access to the names, encrypted passwords, email addresses, physical addresses, phone numbers and dates of birth of the majority of their 145 million members.



Cyber Criminals: Carbanak, 2013 to present – An unknown group of hackers has reportedly stolen USD 300 million from banks across eastern Europe.

Malicious Insiders: A UK-Based Insurer, May 2014 – Hundreds of phones owned by the insurer, were wiped clean when a disgruntled employee of their security contracting firm hacked into one of their systems. In addition to the loss of data, the attack caused the security firm to lose its yearly contract with the insurance company, estimated at potential earnings of GBP 500,000.

The state of cyber crime today

As technology becomes more sophisticated, so too do cyber criminals. They steal money and identities from individuals, and they target businesses of all types and sizes for a variety of end goals. According to PwC[2], the cost of security breaches against business is increasing across the board. For small and medium sized enterprises, PwC estimates the average impact is between GBP 65,000 and GBP 115,000 on average. For larger firms it's GBP 600,000 and GBP 1.15 million. Of course, these are averages and the damage could be higher – especially when you factor in the potential loss of business due to a tainted reputation.

In its 2015 Data Breach Investigations Report (DBIR)[3], Verizon found that cyber criminals were able to compromise an organisation within a matter of minutes in 60% of the cases. That means even if a breach is discovered within hours, the damage may already be done.

Staying informed about what current and growing threats exist is key to understanding what you can do to protect your business, employees and customers.

[1] *http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf*
[3] *To compile data, Verizon worked with nearly 70 contributing organisations includingservice providers, IR/forensic firms, International Computer Security Information Response Teams and government agencies, among others. More than 80,000 security incidents were considered.*

Assessing your exposure

When considering your business's exposure to cyber threats, think about your critical processes and services. Here are a few to consider:

What are your key information systems?

Do you rely on a website for customer orders? If so, do you have robust processes in place to ensure it is secure and can remain available if attacked?

Where is your customer information held? In local databases or a cloud-based system? How are they secured?

Which employees have access to your important business data? Is it necessary for them to have access to everything they do?

Do you rely on any third parties who have access to your critical systems? What checks are there on what they do?

Are your key software and computer systems kept up-to-date with security software, versions and patches?

Does your business regularly use electronic payment systems? What are your processes to avoid fraud through social engineering tactics?

How is email used in your business? Do your employees know how to identify and respond to phishing attacks?

How would you recover should any of your systems be attacked?

Are your employees trained to recognise cyber threats and what to do when faced with them?

The access point: How are they getting in?

Systemic threats: Caused by a weakness of some sort in commonly used technology that hackers and other cyber criminals then use to gain access to victims.

- Heartbleed, 2014 – a vulnerability in one the Internet's most popular security packages allowed perpetrators to access and steal information from the memory of systems using the package.

Staff access & insider: This can be due either to social engineering schemes that set out to trick staff into providing log in information, physical or proximal access using a variety of devices or an actual current or former employee seeking financial gain or revenge.

3rd party & supply chain: In this case, access is obtained through a business partner – whether a supplier, service provider or customer. The tactics used are similar to staff access & insider entry points.

- A large U.S. discount retailer, late-2013: Malicious software installed on point-of-sale (POS) devices in checkout lines led to a breach of personal and financial information for an estimated 110 million customers. Perpetrators were able to hack into the POS devices by stealing the login credentials of a third-party HVAC contractor, which gave them access to the retailer's network.

WHAT IS THE DARK WEB?

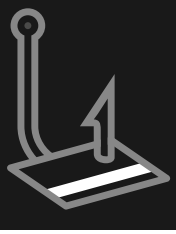
As defined by Dictionary.com, the Dark Web part of the internet that is "intentionally hidden from search engines, uses masked IP addresses, and is accessible only with a special web browser."

TACTICS

Distributed Denial of Service (DDoS): A Global Video and Online Gaming Company, December 2014 – A group of hackers known as the Lizard Squad launched a series of DoS attacks on a variety of gaming sites. As a result, this and other online gaming services experienced several hours-long outages.

Malicious Code: A Large, Multinational Entertainment Corporation, November 2014 – The attack used destructive malware designed to wipe computer hard drives and render data irretrievable. In addition, sensitive operational and personal information, including emails, were released to the public. The company estimates it will spend tens of millions of dollars on investigation and remediation.

Social Engineering: A U.S.-Based For-Profit Managed Health Care Company, February 2015 – Personal information for as many as 80 million customer and employee records were compromised by a sophisticated cyber attack. Early but unconfirmed indications were that attackers may have used social engineering techniques to prompt employees to change their passwords, giving perpetrators access to administrative privileges.



Physical/Proximal Access: A British Multinational Banking and Financial Services Provider, April 2014 – Using a keyboard video mouse (KVM), a team of cyber criminals gained access to and control over accounts at the bank's branches, transferring GBP 1.25 million to cash laundering accounts before being apprehended.

The Perpetrators: who's after you?

Hackers

While stealing money is sometimes a motivation, many hackers are also often in it for the challenge and the potential notoriety they can gain. As such, their skillsets will vary from those who use easily accessed online tools to those who are more technically advanced.

Cyber criminals

Cyber criminals are almost always driven by financial gain. Again, their level of sophistication can range. Lone cyber criminals may take advantage of existing online criminal tools. As they expand their activities, they may also rely on organised cyber crime services – renting or purchasing malware and infrastructure on the Dark Web, for instance, or using backend services such as money laundering. In addition to providing these types of services, organised cyber criminals also use a variety of advanced tactics to launch their own attacks.

Staff access and malicious insiders

Malicious insiders are typically employees or third-party partners who already have access to your organisation's network and abuse their privileges. This includes disgruntled employees who want to harm the company in some way or steal from it.

[1]http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf
[2]To compile data, Verizon worked with nearly 70 contributing organisations includingservice providers, IR/forensic firms, International Computer Security Information Response Teams and government agencies, among others. More than 80,000 security incidents were considered.

The Tactics: how do they do it?

Denial of Service
How much money would you lose if your customers couldn't access your website for an hour? A day? Or more?

If you rely on your website to accept and process orders, the answer is quite a lot. The goal of perpetrators launching Denial of Service (DoS) attacks is to make one or more of an organisation's computer systems unavailable. The most common target is the web server, focused on bringing down the organisation's website and disrupting the flow of business, but can also be used on mail servers, name servers or any type of computer system.

In June of 2014, a well-known code-hosting services provider shut down operations after what began as a DoS attack escalated into a request for ransom. The perpetrator was able to gain access to the company's cloud services and ended up deleting the majority of the company's data, including backups. Although the attack lasted just 12 hours, it was long enough to put the company out of business because, as they stated, "the cost of resolving this issue to date and the expected cost of refunding customers who have been left without the service they paid for..." put them "... in an irreversible position both financially and in terms of on-going credibility."

Malicious code

What if your customer database was stolen?
Based on their estimates, the Verizon DBIR puts the financial loss for a breach of just 1,000 records at between USD 52,000 and USD 87,000.

Malicious code, or malware, can include viruses, trojans and worms. Malware can range in technical sophistication with the ability to evade detection, spread through target systems and carry out a range of activities. Advanced malware, which has not yet been identified as malicious by current anti-virus providers, is becoming more and more common. Malware can be delivered in any number of ways, including:

- Spear-phishing, which uses targeted emails to entice recipients to click on a link and/or enter credentials for delivering malware
- Malvertising, which uses malicious web advertisements inside legitimate websites to deploy malware with the intent of infecting as many internet users as possible
- Watering holes, which focus on targeting specific groups of people by exploiting well-known and trusted websites likely to be visited by their intended victims and redirecting users from the real site to a malicious one

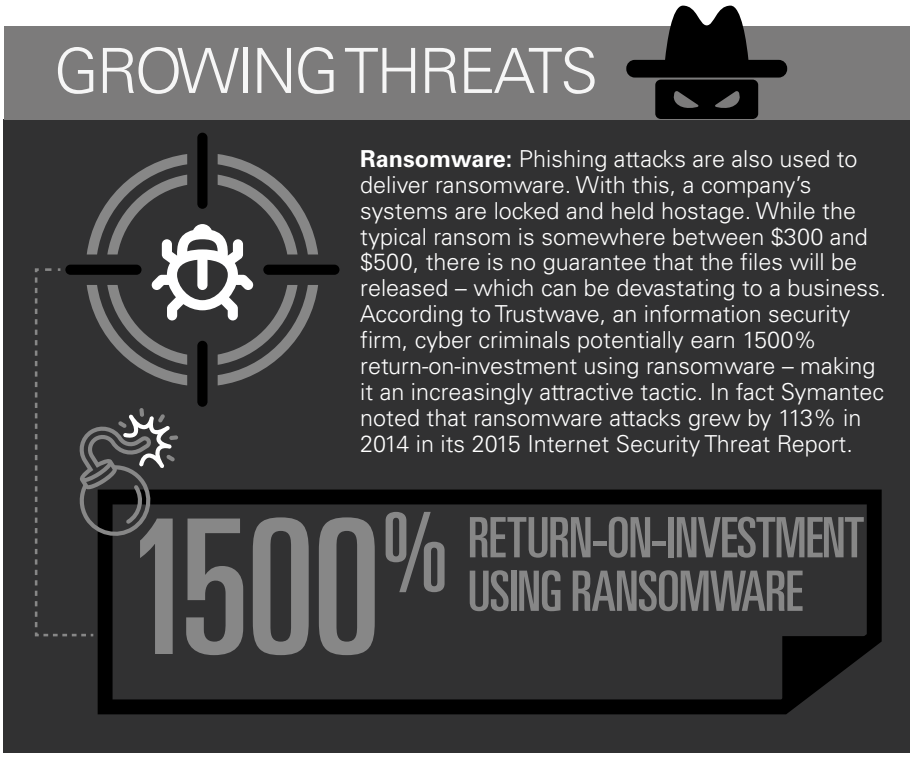
In January of 2015, a small regional U.S not-for-profit healthcare system of hospitals, clinics and community pharmacies discovered some of the corporate workstations and servers had malware installed on them.

The malware allowed perpetrators to capture login information directly from live web sessions when users visited financial and social media websites. Those compromised by the breach include both current and former caregivers.

[3] *http://www.computerworld.com/article/2491008/cloud-security/hacker-puts--full-redundancy--code-hosting-firm-out-of-business.html*

1500%

Cyber criminals potentially earn 1500% return-on-investment using ransomware.



Social engineering

How well educated are your employees about phishing and watering hole attacks?
Social engineering can be passive or active.

- Passive social engineering involves the collection of publicly available information on a victim or organisation, which allows the perpetrator to construct a cyber attack that is more likely to succeed
- Active social engineering uses that information to manipulate targets to take a specific action (clicking on a link, opening an attachment, etc.)

From a business perspective, the ultimate goal of social engineering is to gain access to a protected network or system. Active social engineering is used in spear-phishing and watering hole attacks, which – as noted above – are a means for installing malicious code.

In June of 2015, a 10-year old American networking technology firm discovered that it had lost USD 46 million to a likely social engineering scheme. In their quarterly earnings report[4] they state:

"The incident involved employee impersonation and fraudulent requests from an outside entity targeting the Company's finance department. This fraud resulted in transfers of funds aggregating $46.7 million held by a Company subsidiary incorporated in Hong Kong to other overseas accounts held by third parties."

This type of fraud is becoming increasingly more common and typically targets businesses with overseas suppliers who send payments via wire transfers. Essentially, the email address of one of the business' executives or employees is either spoofed or high jacked and then used to send illegitimate wire transfer instructions to staff responsible for processing such transactions.

[4] https://www.sec.gov/Archives/edgar/data/1511737/000157104915006288/t1501817_8k.htm

Physical/proximal access

How well protected are your systems from unauthorised access?
In this case, perpetrators exploit their ability to gain physical access to your systems to, for example, connect devices such as USB, Keyboard Video Mouse (KVM) and internet-connected devices to your protected computers or network. This gives them access to carry out a range of malicious activity.

Protecting your business: know what you can do

HSBC has long been committed to online security and helping customers protect their businesses against fraud. This includes safeguarding our own systems. That's why our Information Security Teams are constantly monitoring activity across the entire Bank, as well as researching evolving cyber crime tactics to combat the perpetrators.

However, the security of your systems and information is a shared responsibility. Although cyber criminals are always inventing new ways to infiltrate systems, perpetrate fraud and steal money – there are several steps you can take to minimise the risk of an attack.

Make use of industry-standard solutions
Start with a "defence in depth" security protection strategy by installing and updating anti-virus software and firewalls as well as separate email protections and internet proxy services.

Keep hardware and software up-to-date
Be sure to update software and operating systems on every company-owned computer as soon as vendors release new versions. This includes downloading security patches immediately if they are updated in between releases.

Similarly, don't forget to upgrade hardware devices such as wireless routers. Vulnerabilities in internet-connected hardware can be exploited from anywhere in the world. It's also important to ensure that any mobile devices like laptops and smartphones used for business purposes are encrypted.

Train employees on best practices
Giving your employees the information they need to keep business systems and information safe is key. Educate them on existing cyber threats and keep them up-to-date with new ones that may impact your industry using trusted resources. (Please see the additional resources section).

Train staff never to open attachments or click on embedded links in emails originating from unknown sources. When they do receive a suspicious email, it's best to delete it without opening it. If an email appears to be from a trusted partner and asks for secure information such as login credentials or to reset a password – have employees report it to your security team as well as the partner's.

Employees should also never download unauthorised software programmes, documents or applications directly from the web.

REMEMBER

No bank or service provider, including HSBC, will ever send emails requesting confidential details such as bank account numbers or other sensitive information.

Establish policies around security protocols

Many companies put a secure password policy in place so that passwords have a certain level of complexity. As an example, you may want to require that passwords be at least eight characters in length and include at least one number, capital letter and/or symbol. It's also prudent for employees to change passwords periodically, once every three or four months.

Ensuring employees only have access to the systems and information they need to do their jobs can lessen exposure to insider threats. Dividing financial responsibilities among key staff members may also help minimise the risk of internal fraud. This includes implementing a "maker/checker" process for payments where one staff member initiates a transaction and another approves it.

Restricting internet access on business network connected machines to only trusted sites and services can protect your systems from potential malware infection from compromised websites. Limiting or eliminating the use of external media such as USB sticks will further reduce the risk of data theft and infection from malware.

Regular security analyses – such as testing websites and internet facing applications, conducting security assessments of business information assets and maintaining up-to-date inventory – may uncover weaknesses. In addition, putting disaster recovery systems in place that include backups to all major systems and information assets as well as regular testing will also help protect against data loss.

Take precautions with external partners

Conduct thorough background checks on all third party suppliers with whom you work and review contracts periodically to ensure they are current. Pay special attention to those who have access to or provide your IT systems such as technical support contractors or Cloud services.

Warding off cyber criminals – a checklist

While not an exhaustive list that may not apply in all cases, following are a few actions to consider in protecting yourself against cyber crime:

- Install and update anti-virus software as well as firewalls, email protections and internet proxy services
- Keep software and operating systems up-to-date by downloading new releases and security patches as soon as they are available
- Upgrade internal hardware devices that may have become obsolete and ensure mobile devices used for business are encrypted
- Hold regular training sessions to inform employees of what to look for in terms of existing and growing threats
- Put policies in place that further protect your systems and information by giving staff guidelines for conducting business online
- Limit access to systems and information based on job duties, and split financial responsibilities across two or more employees
- Restrict internet access to trusted websites and limit the use of external media devices
- Conduct regular security testing and assessments of websites, internet facing applications and information assets
- Establish and test disaster recovery plans and backups for all critical systems and information assets
- Have a dedicated incident management team and/or protocols in place
- Thoroughly research the background of all third party providers and ensure robust contracts are in place

Additional resources

Since cyber crime is constantly changing, it's important for you to stay up-to-speed on what's happening in the industry and what you can do to protect your business. For more information:

- Download Verizon's 2015 Data Breach Incident Report[5]
- Read through the UK Government's "Small businesses: What you need to know about cyber security[6]"
- Take the online course, "Cyber security for small business[7]," from the U.S.'s Small Business Administration (SBA)
- Create a cyber security plan using the FCC Small Biz Cyber Planner[8], developed by the U.S.'s Federal Communications Commission (FCC)
- Conduct a "Health Check" on your devices, computers and website with the guidance of Hong Kong's Cyber Security Information Portal's Safety Centre[9]
- Have employees take McAfee's Phishing Quiz[10]

[5] *Links to http://www.verizonenterprise.com/DBIR/2015/*
[6] *Links to https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/412017/BIS-15-147-small-businesses-cyber-guide-March-2015.pdf*
[7] *Links to https://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses*
[8] *Links to https://www.fcc.gov/cyberplanner*
[9] *Links to http://www.cybersecurity.hk/en/index.php*
[10] *Links to https://phishingquiz.mcafee.com/*

More Information

Following please find sources for more information on the examples included in this document.

Anthem
http://www.nbcnews.com/news/us-news/anthem-major-health-insurer-suffers-hack-attack-n300511

Aurora Health Care
http://www.ago.vermont.gov/assets/files/Consumer/Security_Breach/Aurora%20Health%20Care%20SBN%20to%20Consumer.pdf

Aviva
http://www.bbc.co.uk/news/technology-34052408

Barclays
http://www.bbc.co.uk/news/uk-england-london-27146037

Carbanak
http://securityaffairs.co/wordpress/33565/cyber-crime/carbanak-swipes-300m-banks.html

CodeSpaces
http://www.computerworld.com/article/2491008/cloud-security/hacker-puts--full-redundancy--code-hosting-firm-out-of-business.html

Codan
http://www.smh.com.au/business/codan-fights-back-after-chinese-hackers-stole-metal-detector-designs-20150624-ghx36t.html

eBay
http://www.nytimes.com/2014/05/22/technology/ebay-reports-attack-on-its-computer-network.html

Heartbleed
http://www.bbc.com/news/technology-27058143

Sony
http://www.bbc.co.uk/news/technology-30530361

Target
http://money.cnn.com/2014/02/06/technology/security/target-breach-hvac/index.html

Ubiquiti Networks
http://krebsonsecurity.com/2015/08/tech-firm-ubiquiti-suffers-46m-cyberheist/

Xbox
http://www.businessinsider.com/xbox-live-outage-may-be-from-lizard-squad-hack-2014-12?op=1