KEEPING YOUR COMPANY CYBER SAFE

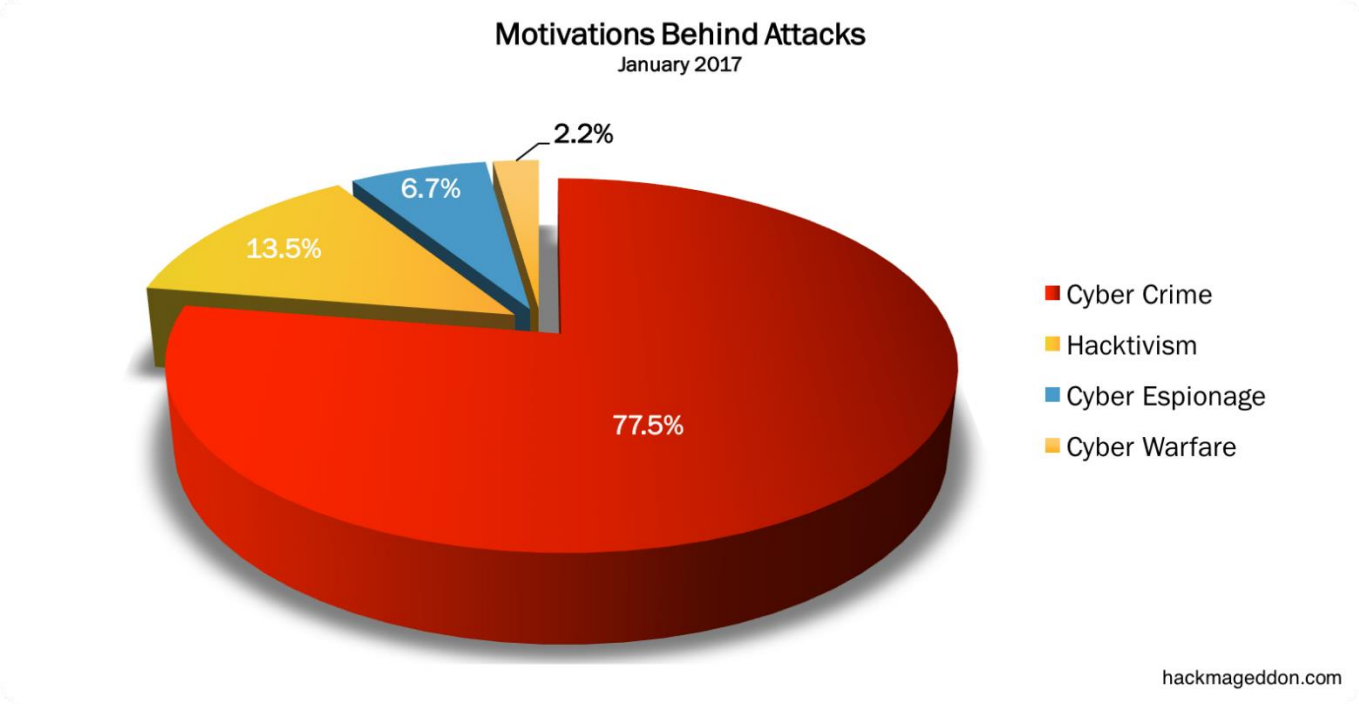
White Paper

By Robert Ek

Table of Contents

Executive Summary

This paper focuses on 2 areas. Firstly, it informs business owners of the current landscape of Cyber Security. This includes the increasingly sophisticated tools cybercriminals are now using to access private information. Secondly, it discusses the Australian Government's new approach to the public disclosure of Data Breaches (coming into effect February 2018).



Introduction

Statistics indicate that $3,000 is the average loss from a burglary. The largest loss on record from a bank heist in the Western World is documented at $38,000,000. However, these figures pale in comparison to the staggering $570,000,000,000 the global economy loses to cybercrime each year. As we can see from chart, Cybercrime constituted the bulk of Cyberattacks in 2017.

Research conducted by the National Cyber Security Alliance found that:

- Almost 50 percent of small businesses have experienced a cyber-attack
- More than 70 percent of attacks target small businesses
- As much as 60 percent of hacked SMEs go out of business after six months

These attacks are taking a huge toll on our economies. It is imperative cyber security becomes a part of our organisational dialogues.

Security Issues: The Current Landscape

Cybercrime cost the global economy more than US$450 billion in 2016. The WannaCry ransomware attack alone, which crippled computers in over 150 countries in May, cost $4 billion according to certain estimates. (Hiscox, 2017)

Corporations have realised how vulnerable and defenceless they are when attacked by small groups of people on the other side of the globe. Unfortunately, expensive security systems and information security consultants don't faze hackers - they have the resources to mount assaults. In a New York law-firm's case, prosecutors said the attackers attempted to penetrate targeted servers more than 100,000 times over seven months, ultimately netting $4m USD.

Cybercrime is rapidly increasing for the same reason online services have become so popular with consumers and businesses alike: easy-access technology. Hacking is easier than ever thanks to the ever-growing number of online targets and the proliferation of off-the-shelf attack software. The Internet networks that were built with convenience and profit in mind, are now exposing their users to a stream of new threats.

Our company, Go Systems, recently conducted forensic analyses for two clients who fell victim to 'inside jobs'. In the first instance, employees managed to hack their company's database, retrieving sensitive information and consequently, a substantial amount of funds. In the second instance, the firm received a seemingly innocuous email with a Dropbox link asking for usernames and passwords. One simple click. Disastrous consequences for the firms.

In both examples, the cybercriminals spent significant time gathering intelligence and collecting multiple usernames. They learnt how bank transfers were conducted and hacked their websites to put in dummy pages.

To address these issues, we've evolved from being a **MSP** (Managed Service Provider for Infrastructure, Cloud, Apps, desktop and mobility etc.) to being a **MSSP** (Managed Security Service Provider).

Cybercriminals have proved adept at adopting successful corporate strategies of their own. A recent development has seen clever crooks selling hacking tools to the lowest rank of criminals. According to a report from a security software giant, gangs now offer so-called RaaS (Ransomware as a Service), a trick that involves licensing software that freezes computer files until a company pays up. They then take their cut for providing the license to their criminal customers.

It's time to seal the hatch. We are seeing more and more attacks, and they will only continue to grow in frequency and sophistication.

So how can you ensure your website is secure from hacking?

What does the average business owner understand? Not enough! They're not getting the right information from their tech team. The discussion needs to cover all bases and business owners need a team that can provide a complete picture and keep regular updates.

There are three areas you must address to reduce the exposure of your business to Cyber Risks.

1. **The four layers of Security** – Firewall (gateway to the internet), Endpoint (desktop/laptop), Cloud (email) and Web (filtering). Each with different vendors who are all market leaders.

2. **Your staff** – the Internal weak link. This could be malicious or accidental loss of data. PCS and SOC can assist with this (more on this below).

3. **Monitoring the business 24/7** - using a live SIEM (Security Information and Event Management) platform in a SOC (Security Operation Centre) running 24/7.

SOC (Security Operations Centre) specialise in monitoring clients' sites who want it on a 24/7 basis; eyes on screens look for alerts.

Go Systems also have a solution for a PCS (People Centric Security) approach to educate staff through policy and warning screens on the use of data held by the business.
Every staff member needs to understand their responsibilities and be extra cautious, for the safety of themselves and your business. This is: Business Security starts with employees who need to be prepared to assist in keeping the business computers and network safe.

Security Update - Mandatory Data Breach Notification

Data breaches (including lost or stolen data) are a fact of modern life. It's estimated that more than 9 billion data records have been lost or stolen worldwide since 2013. Therefore, businesses are encouraged to develop a robust cybersecurity framework, data breach policy and response plan to ensure compliance with the law.

From 22 February 2018, it will be mandatory for businesses to notify the Office of the Australian Information Commissioner (OAIC) and any affected individuals in certain circumstances if the business suffers a data breach.

The rationale underpinning these requirements is to enhance the protection of personal information held by businesses and to enable individuals to mitigate any harm caused by a data breach.

Overview

To comply with the requirements of the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) (Privacy Amendment Act), relevant businesses must give formal notice if:

- There are reasonable grounds to believe an "eligible data breach" has occurred; or
- The Australian Information Commissioner (the Commissioner) believes on reasonable grounds that an "eligible data breach" has occurred and directs that business to give notice.

Accordingly, while a direct selling business or distributor will not ordinarily be required to comply with the Privacy Act, they will need to yield if they collect health information from customers and distributors in their downlines.

What is an "eligible data breach"?

An eligible data breach is where there is unauthorised access to, or disclosure of, personal information or where loss of this information - in circumstances where it is likely to occur - would likely result in "serious harm" to any individuals to whom the information relates.

What is "serious harm"?

Serious harm is assessed according to the standard of the reasonable person. It can be physical, psychological, emotional, economic, financial or reputational. However, an individual upset or distressed on its own is unlikely to constitute serious harm.

To assess whether unauthorised disclosure or access would be likely to result in serious harm, considerations include:

- the nature of the information and its sensitivity, e.g. health information or credit card details
- whether the information is protected by one or more security measures
- the likelihood that any of those security measures could be compromised
- whether security technology was used to make the information unintelligible or meaningless to unauthorised persons; and
- the likelihood that a person has obtained or could obtain information or knowledge to circumvent the security technology.

The statement must include:

- the identity and contact details of the business
- a description of the data breach
- the kinds of information concerned
- recommendations about the steps that individuals should take in response to the data breach.
- A copy of the statement must be given to the Commissioner.

The business should then notify individuals to whom the information relates to or is at risk from the breach as soon as the business is aware that there are reasonable grounds that an eligible data breach has occurred. Direct selling businesses may use their usual method of communication when notifying an individual. If it is not practicable to inform individuals, they must publish a copy of the statement on their website and take reasonable steps to publicise the statement's contents.

What are the consequences for contravening the Privacy Act?

Failure to comply with the Privacy Act may be considered as interference with the privacy of the individual. For a corporation, the maximum civil penalty that can be imposed for a serious breach, or for multiple breaches, of the Privacy Act is $1.8 million. Also, a corporation may be ordered to compensate an individual for loss or damage caused.

Data breaches from direct selling organisations can also cause significant damage to the organisation's reputation as well as cause business interruption and loss. Company directors are responsible for cybersecurity issues and could be found to be personally liable.

Is your direct selling business (products or services) prepared to handle a data breach?

- Does your business (and independent distributors) collect sensitive information, such as financial or health information?
- Do your independent distributor agreements and Policies and Procedures contain privacy obligations?
- Are your independent distributors required to notify you of any suspected data breaches?

These are all matters which you should consider when determining whether your business and your independent distributors are taking reasonable steps to ensure privacy compliance.

The security measures and technology used by a business are essential factors in determining whether a data breach has caused or is likely to cause serious harm, which demonstrates the need for direct selling businesses to be better protected and insulated from cyber risks.
Your business needs to explore strategies to enable the development of a robust cybersecurity framework. Not only will this protect your commercial interests, but it will also ensure that you are prepared to comply with the Privacy Act by 2018.

The OAIC's guide to developing a data breach response plan was published in April 2016. The guide is being updated to reflect the changes introduced by the amendments to the Privacy Act.

February 2018 is fast approaching; make sure your clients and your business are prepared!

Appendix: Ensuring Compliance with Privacy Act 1988 and Mandatory Data Breach Reporting

Compliance relates to your staff as part of the developed framework. This refers to meeting the requirements of the Privacy Act and the Mandatory Data Breach Reporting amendments (2016).

'Understanding and ensuring compliance to the privacy act 1988 And mandatory data breach reporting (privacy amendment bill 2016) using a compliance service'

Entities covered by the Australian Privacy Act 1988 have obligations under the Act to take reasonable steps to protect personal information held, from misuse, interference and loss, and from unauthorised access, modification or disclosure. The Privacy Amendment (Notifiable Data Breaches) Bill 2016, establishes a mandatory data breach notification scheme in Australia.

A Compliance Service (CS) not only facilitates compliance with the Privacy Act by providing reasonable protection of personal data under the Australian Privacy Principles but also contains necessary ISO27001 processes to enable the review and where appropriate, escalation of incidents on a case-by-case basis.

Privacy Act 1988

The 'Guide to securing personal information' published by the Office of the Australian Information Commissioner provides guidance on the reasonable steps entities are required to take under the Privacy Act 1988 to protect the personal information they hold from misuse, interference, loss, and from unauthorised access, modification or disclosure.
Using a CS addresses the following 9 areas to providing strong protection against data breaches.

1. **Governance, culture and training**.

The CS implements a People Centric Security (PCS) approach in which end users are educated through policy and warning screens on the use of personal data

2. **Internal practices, procedures and systems.**

The CS implements ISO27001 processes including the necessary separation of roles with respect to data ownership, protection, review and management oversight

3. **ICT security.**

The CS mitigates the risks of internal/external attackers and human error whilst allowing users to continue work uninterrupted

4. **Access security.**

The CS provides access controls on personal data within encrypted documents to ensure only authorised users can access the data.

5. **Third party providers including cloud computing.**

The CS tracks the outflow of personal data to cloud applications and websites including Office365, Dropbox, Google Docs, etc. and secures it using encryption

6. **Data breaches.**

The CS provides full visibility of potential data breaches and the necessary workflow to enable further investigation of the same.

7. **Physical security.**

The CS provides full auditing facilities including a Hardware asset audit so that missing devices can be quickly identified.

8. **Destruction and de-identification.**

The CS provides extensive data discovery functionality allowing the organisation to locate personal data stored within the organisation and so facilitate the destruction of the same.

9. **Standards.**

The CS implements the ISO27000 family of processes to ensure all personal data is identified, protected and any potential data breaches are managed in accordance with the standards specified by the Office of the Australian Information Commissioner.

Functionality includes:

- Application, device and network blacklisting
- Monitoring personal information within communications, its usage within applications and its movement across the network
- Automatic encryption of documents containing personal information, along with the provision of applications to allow mobile workers and collaborating organisations to access them where required

Mandatory Data Breach Reporting (Privacy Amendment Bill 2016)

The 'Guide to developing a data breach response plan', recently released by the Office of the Australian Information Commissioner, defines an ideal plan in the steps listed below. The functionalities and workflow provided by the Compliance Service facilitate these steps.

1. **Contain the breach and do a preliminary assessment.**

- The CS identifies the users and channels involved in a breach so that further actions of the users can be contained via its data protection functionality, which includes application, device, network blacklisting and data encryption.
- The CS enables a preliminary assessment to be conducted by specifying the personal information involved as well as the cause and extent of the breach.
- Where necessary, the CS enables the breach to be escalated to the relevant internal authorities via its case management workflow functionality. The CS implements ISO27001 processes including the necessary separation of roles concerning data ownership, protection, review and management oversight.

2. **Evaluate the risks associated with the breach.**

- The CS provides the necessary information including the type of personal information involved, the context the information appeared in and the extent of breach.
- The CS 'case management workflow' functionality enables communication between the internal authorities and those tasked with identifying data breaches and allows further information and related incidents to be gathered together in the same case to facilitate decision making.

3. **Notification.**

- The 'case management' functionality provides all the necessary detail required to make a notification to the Office of the Australian Information Commissioner.

4. **Prevent future breaches.**

- The outcome of the investigation can be returned to those administering the CS to allow appropriate settings to be modified preventing further breaches.

If you would like to discuss your Cyber Security, please contact Go Systems

Go Systems Pty Ltd

Cloud Solutions - IT Services - Security

1300 786 746

sales@gosystems.com.au

www.gosystems.com.au