Grant Thornton
An instinct for growth™

The Realities of Cybersecurity Risk

An update from the front lines

Sandy Boucher
National Cybersecurity Leader

The cybersecurity risk landscape

Who is out there?
- Amateur
- Low end
- Org. Crime
- National

What are they after?
- Financial
- Ideological
- Revenge

Sophisticated attacks
- Banking related attacks
- Extortion demands
- Mass PII thefts

Internal
- Accidents/careless
- Deliberate

Key vectors of attacks
- Hack
- Click

Implications for victims
- Financial loss
- Reputational damage
- Business interruption

How organizations can protect
- Risk assessment
- Common sense steps

Who is out there? - Cyber threat actors

Early hacker

Cyber mischief

- Penetrating systems for "sport" and ranking
- Simple malware/viruses for notoriety/"phun"
- Low scale reverse engineering for piracy

Hacktivists

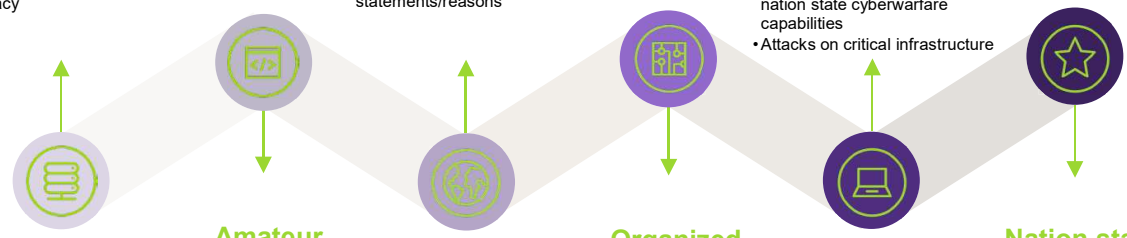
Cyber hacktivism

- Use of DDoS/Botnet malicious tools to deny access to internet services for political reasons/statements
- Site defacements for political statements/reasons

Terrorists

Cyber terrorism

- Currently more focussed on using internet/social media for psyops and infowarfare
- Can also operate as hacktivists
- High interest exists in developing nation state cyberwarfare capabilities
- Attacks on critical infrastructure



Amateur cyber criminal

Low level cybercrime

- One-off data theft
- Piracy for profit
- One-off frauds
- Uncoordinated attacks
- Purchase tools

Organized cyber criminal

High level cyber crime

- Professionally engineered malicious tools
- Advanced/multi-stage system/network penetrations
- Established relatively liquid markets for selling stolen IDs
- High value industrial espionage
- Legal and political immunity
- Significant measures

Nation state

Cyber warfare

- Highly advanced tools/methods
- Currently most actions based on large scale intelligence gathering and industrial/economic espionage
- Cyberwarfare capabilities to target and attack critical infrastructure (e.g. power grid, water, manufacturing, financial, telecom, etc.)
- Currently used as means of standard military doctrine and for economic espionage

Most common types of cybersecurity breaches

Phishing

Attacker sends email containing malware

Spear phishing/ Whaling

Targeted phishing attacks against a specific individual or organization

SQL injection

Malicious code added into website to steal user names and passwords

Cross-Site Scripting (XSS)

Malicious code added to a website in order to attack individuals who visit the site

Denial of Service (DoS)

Attacker floods a server with more traffic than it can handle causing it to shut down

Man-in-the-Middle

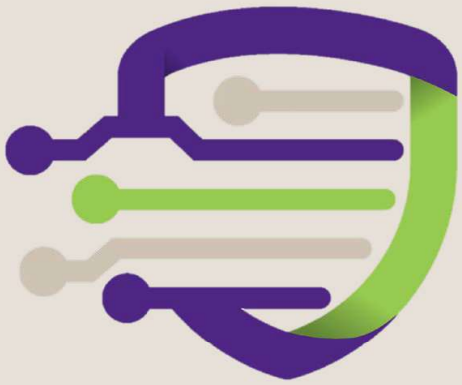
Attacker places themselves between you and your web session allowing them to take over your activity

Credential Sale/Reuse

Attackers use stolen credentials to access user accounts

What we are seeing

Cyber awareness is very low for both management & employees	Most of the victims had no real understanding of the full impact hat an attack would have on their operations	Low level of knowledge on cyber insurance	Most victim organizations did not have appropriate data backup
Many victims placed undue reliance on underqualified outsourced IT contractors	Almost all victims had not taken even the easiest logical steps to enhance their security	In more sophisticated hacks, time to discovery is months or longer	An alarming number of victims did not have commercial AV software



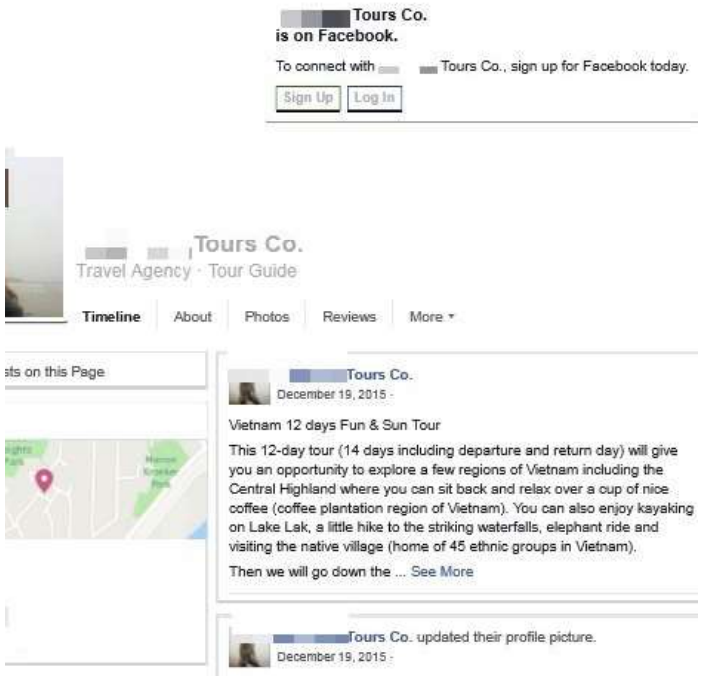
Case study #1: Ransomware

Guided analysis of a real ransomware case from a GT client

Case 1: Ransomware attack – the company

Who	What	When	How
Best RV: small BC based RV sales company 17 employees in Vancouver and interior BC	Remote office is connected to the server by a remote desktop function Simple IT setup services provided by a local firm	Mid May 2017 Just before the key sales season	One employee thinks she may have clicked on an email attachment that was strange

Case 1: Ransomware attack – additional information



Missing IT provider located in Vietnam

Case 1: Ransomware attack – AV systems history

Installation dates

AV software Vendor

	B	C
	AV Involved	Date
	AVG	20150315
	AVG	20150629
	AVG	20150629
	AVG	20150629
	AVG	20150629
	VIPRE	20150723
	AVG	**20150723**
	AVG	**20150723**
	AVG	**20150723**
	AVG	**20150723**
	AVG	**20150723**
	Malwarebytes	20150727
	Kaspersky	20150902
	Kaspersky	20150902
	HitmanPro	20150902
	F-Secure	20150902
	AVG	20151224
V	VIPRE	20160324
		20160407

Case 1: Ransomware attack – breach history & country

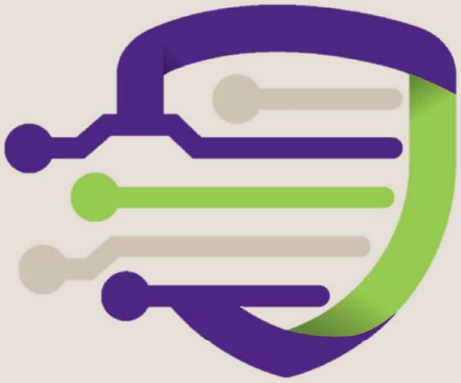
IP address and country of breach

Source Network Address:	CountryName
91.224.160.26	Netherlands
175.9.80.49	China
191.101.31.126	Netherlands
175.13.158.170	China
220.168.13.38	China
220.168.15.243	China
46.148.22.10	Ukraine
46.161.40.11	Russia
122.147.187.126	Taiwan
188.72.105.46	United Kingdom
182.99.224.35	China
182.99.224.35	China
46.161.40.11	Russia
178.34.158.226	Ukraine
46.148.22.10	Ukraine
94.41.117.219	Russia
220.161.133.218	China
46.148.22.10	Ukraine
193.169.86.10	Ukraine
37.57.0.195	Ukraine
182.87.152.237	China
77.79.136.15	Russia
113.243.136.189	China
117.164.245.198	China
182.110.240.29	China
182.110.240.29	China
193.169.86.10	Ukraine
193.169.86.10	Ukraine
193.169.86.10	Ukraine
79.141.163.18	France
82.114.86.91	Albania

Case 1: Ransomware attack – outcome

Cause identified ✓ **Data recovered** ✗ **Malware removed** ✓ **Cybersecurity status** ?

1. System breached through remote desktop service, used by client for smaller office
2. Router was not properly configured AND no proper firewall used
3. Multiple hackers able to breach security with brute force attack
4. Initial breach symptoms not properly understood by management
5. Eventually lost all their data at critical time of year AND required a complete rebuild
6. Unable to access any systems including payroll, email, client management software etc.



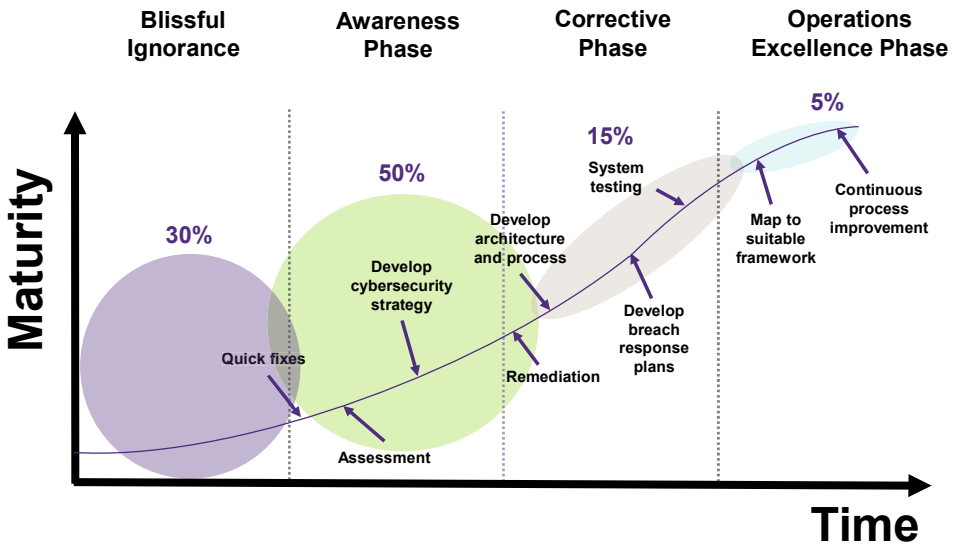
A simple Approach to cybersecurity

Domains and functions of cybersecurity

- Governance
- Cyber risk assessment
- Business resilience and system security
- Data security management and privacy
- Security standards compliance
- Identity and access management
- Third party assurance
- Application security
- Physical security
- HR security
- Incident response and investigation

1

Cybersecurity maturity continuum



Source: Gartner

Overview

Cyber Incident Response

A data breach can be a real danger but being prepared can help you mitigate the damage from and attach

43%
OF COMPANIES EXPERIENCE A DATA BREACH

63%
OF THESE DID NOT HAVE AN INCIDENT MANAGEMENT PLAN

56%
DO NOT HAVE POLICIES THAT CLARIFY WHAT WEBSITES EMPLOYEES CAN USE

60%
CLOSE PERMANENTLY WITHIN 6 MONTHS

90%
CLOSE PERMANENTLY WITHIN 2 YEARS

How do I prepare my organization for a breach?

BEFORE

- Form an incident response team (IRT) and plan of action
- Map and classify the organizations data
- Conduct a vendor assessment
- Create a risk profile that contemplates all relevant privacy risks
- Cyber insurance

What do I do if a breach occurs?

Mobilize IRT and initiate action plan:

- Engage outside counsel
- Contact outside forensic team
- Contact PR group
- Conduct investigation of the breach

DURING

What is the best way forward after a breach?

AFTER

- Monitor to detect future anomalies
- Remediate any gaps discovered during the investigation
- Establish regular reporting to executive management
- Remediation

Grant Thornton's Incident Response Services

- Breach response
- Forensic investigation
- Breach coaching
- Breach response planning
- Litigation support
- Remediation advice

National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc

National Cyber Security Centre
a part of GCHQ

Cyber Security Small Business Guide

This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at www.ncsc.gov.uk/smallbusiness .

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

Identify what needs to be backed up. Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.

Ensure the device containing your backup is *not* permanently connected to the device holding the original copy, neither physically nor over a local network.

Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than "desktop" equipment.

Switch on PIN/password protection/fingerprint recognition for mobile devices.

Configure devices so that when lost or stolen they can be tracked, remotely wiped or remotely locked.

Keep your devices (and all installed apps) up to date, using the 'automatically update' option if available.

When sending sensitive data, don't connect to public Wi-Fi hotspots – use 3G or 4G connections (including tethering and wireless dongles) or **use VPNs.**

Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

Use antivirus software on all computers and laptops. Only install approved software on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.

Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the 'automatically update' option where available.

Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.

Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

Ensure staff don't browse the web or check emails from an account with Administrator privileges. This will reduce the impact of successful phishing attacks.

Scan for malware and change passwords as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).

Check for obvious signs of phishing, like poor spelling and grammar, or low quality versions of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords – when implemented correctly – are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

Make sure all laptops, Macs and PCs **use encryption products that require a password to boot. Switch on password/PIN protection or fingerprint recognition** for mobile devices.

Use two factor authentication (2FA) for important websites like banking and email, if you're given the option.

Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).

Do not enforce regular password changes; they only need to be changed when you suspect a compromise.

Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.

Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.

Consider using a password manager. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

For more information go to www.ncsc.gov.uk @ncsc

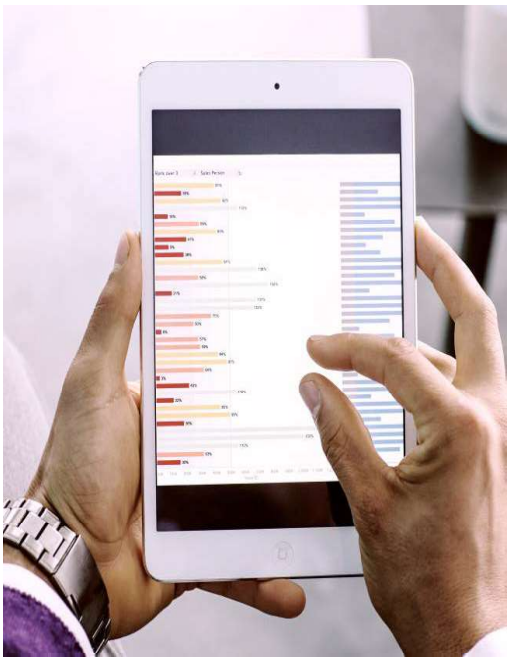
Start the Cybersecurity conversation at your organization

Cybersecurity isn't just a technology issue, it's about business risk, organizational culture, and education

Mandatory data breach reporting Nov 1, 2018

10.1 (1) An organization shall report **to the Commissioner** any breach of security safeguards involving personal information under its control if it is **reasonable in the circumstances** to believe that the breach creates a **real risk of significant harm** to the individual

10.1 (3) – requires you to also notify the individual in the same circumstances



Thank you

Questions?

Sandy Boucher

Senior Investigator
Advisory Services, Forensics
Grant Thornton LLP.
T: +1 416 369 7027
E: Sandy.Boucher@ca.gt.com
www.linkedin.com/in/sandyboucher/
https://twitter.com/oldplod