



THE MALAYSIAN
INSURANCE INSTITUTE



CYBER RISK INSURANCE

Presented by:

Roy Sharma

Managing Director / Principal Officer
Asia Reinsurance Brokers (Labuan) Ltd

Part 1 – Overview



Cyber Risks

The increasing use of technology and the Internet in all aspects of daily life puts everyday citizens as well as business at risk of becoming targets of cybercriminals.

As society comes to rely more and more on the Internet, the dangers posed by different types of cybercrime have become very real threats. These threats come in a variety of forms and target different features of the Internet, technological devices and their users.

As a result, cyber threats are constantly evolving and changing and the approach to the exposure needs to evolve as well.



Cyber Risks

Despite the best efforts of companies and organizations to minimize the impact they are often let down by the need to constantly adapt to the changing threat, the speed of change in technology, or even good old fashioned human error.

Fortunately there is a solution.....Cyber Liability Insurance.



"I'm no expert, but I think it's some kind of cyber attack!"



Cyber Risks

What security threats did companies face in 2016?

In Q3 2016 alone, 18 million new malware samples were captured. That's an average of 200,000 per day. And that's only the malware samples detected by one company.

More than 4,000 ransomware attacks have occurred every day since the beginning of 2016. That's a 300% increase over 2015, where 1,000 ransomware attacks were seen per day.

Phishing and Overconfident Users

78% of people claim to be aware of the risks of unknown links in emails. And yet they click anyway.



Cyber Risks

52% of organizations that suffered successful cyber attacks in 2016 aren't making any changes to their security in 2017.

Copyright 2004 by Randy Glasbergen.
www.glasbergen.com



"The boss is worried about information security,
so he sends his messages one alphabet letter
at a time in random sequence."



Cyber Risks

The most expensive computer virus of all times cause damage worth \$38.5 billion!

Mydoom was mainly transmitted by email, disguised as spam email. A user might inadvertently open the attachment in the email and the worm would re-send itself to every address it could find.

Despite Donald Trump's approach to many things in the media "This is not Fake News"



Cyber Risks

The US Navy receives 110,000 cyber attacks per hour.

More importantly for business operations, potentially its people are the weakest link. There are currently 1.6 Billion social network users accessing online social media.



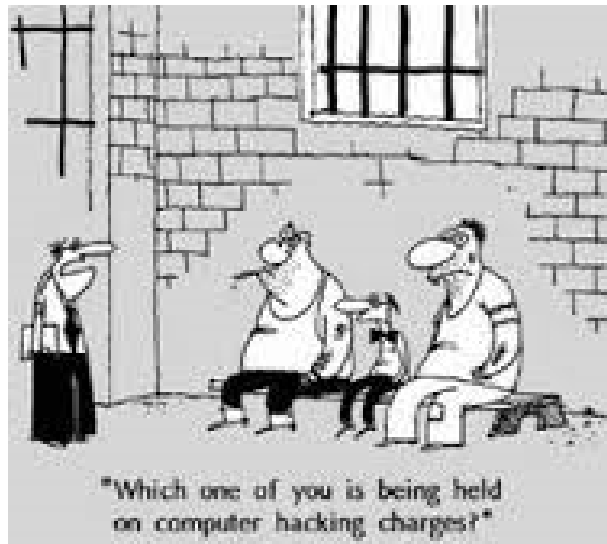
Cyber Risks

Despite what Trump may tell you. This is not public enemy number 1 with regards to cyber risks.

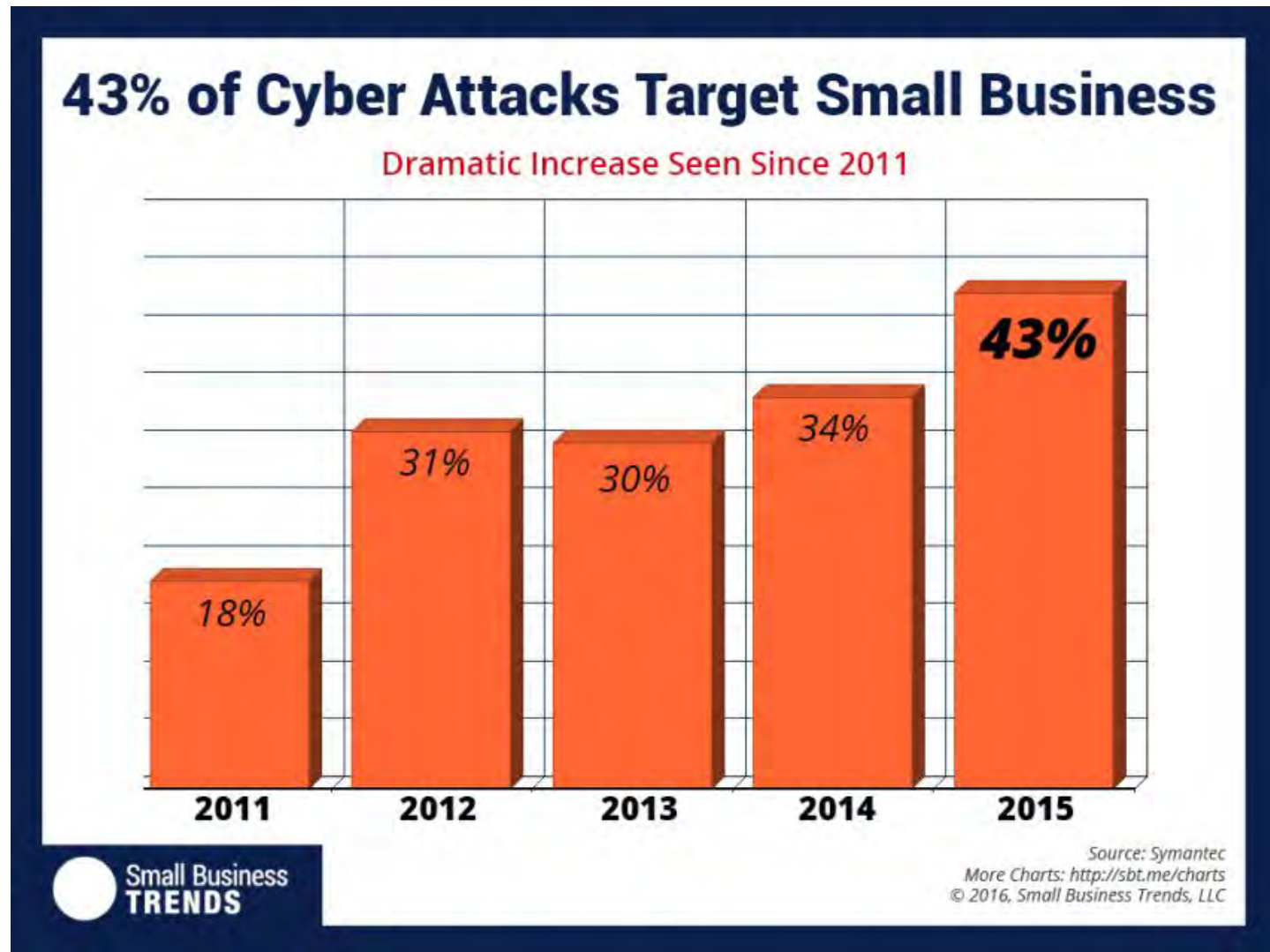


Cyber Risks

This is more likely the culprit!!!



Forget Big Business - Small Business is now increasingly under threat.....



Cyber Risks

Realistically the larger corporations often have up to date firewalls, encrypted protection protocols as well as in-house IT operations to respond to a threat scenario. In addition they will often have the financial capability to cover and protect their losses.

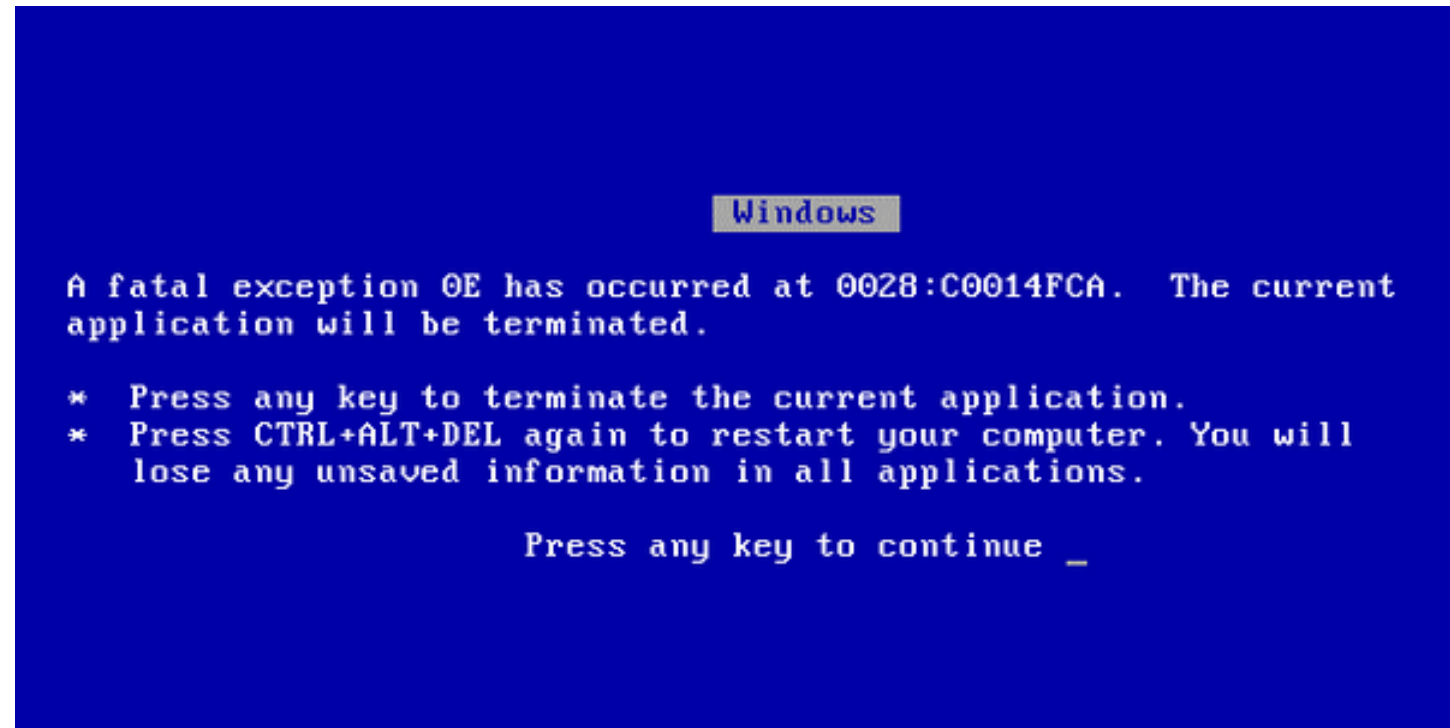
Can the same be said of the smaller SME operations who often use outdated software and firewalls, external IT providers and do not have the financial capability.

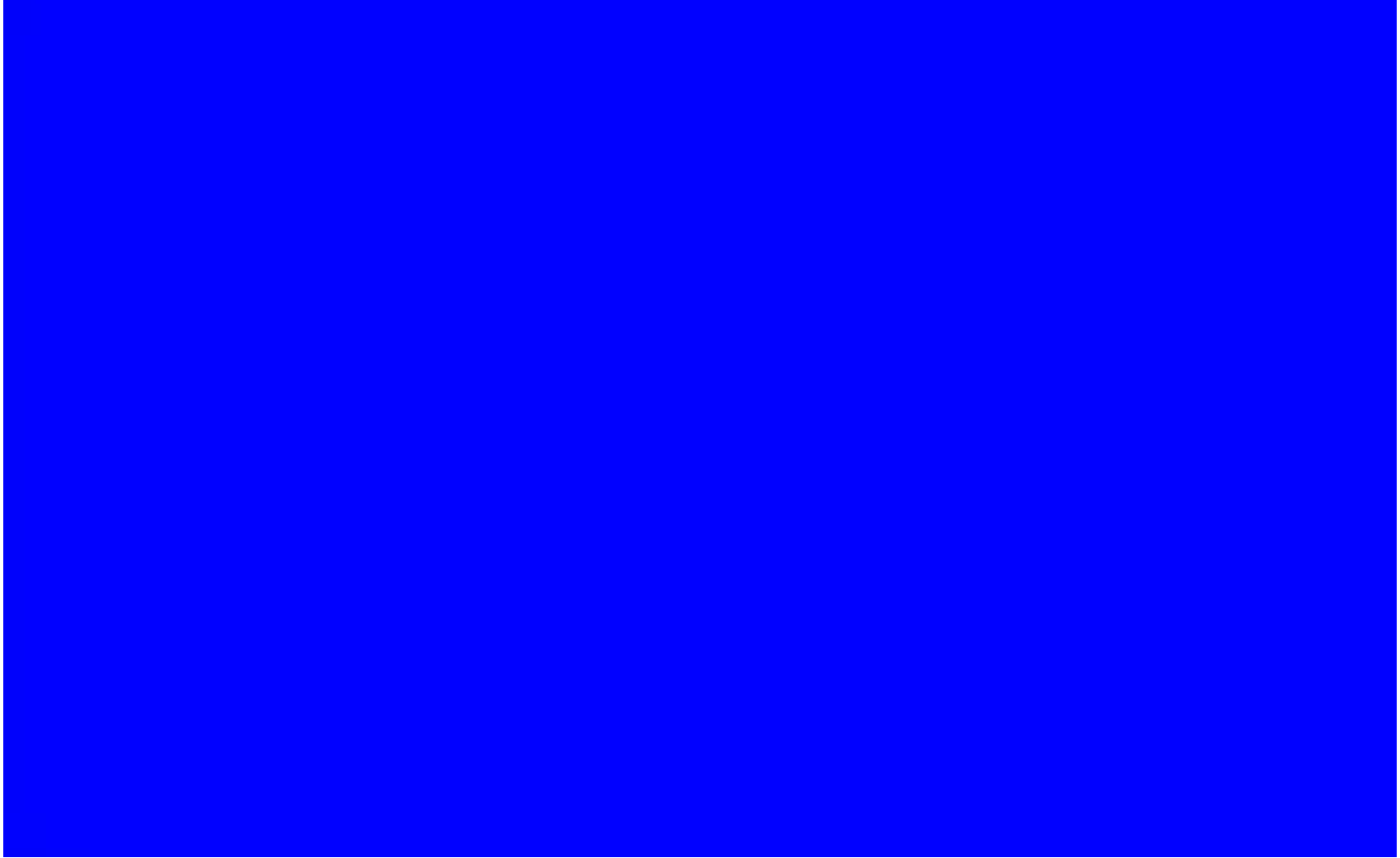
These are the companies that need to purchase cyber insurance....now more than ever before.



Cyber Risks

So if you don't want this to happen to one of your clients, then please listen carefully and consider the options.



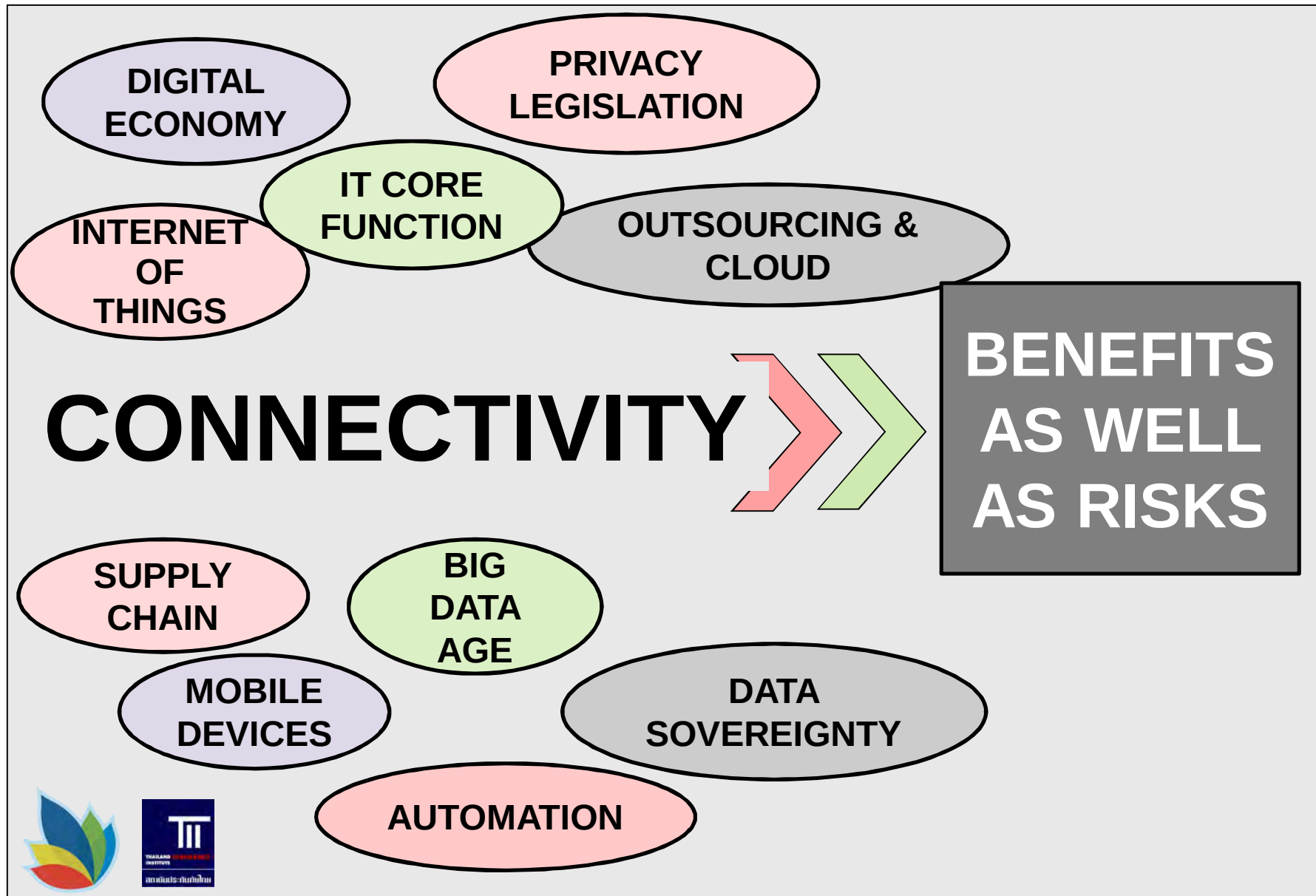


PART 2



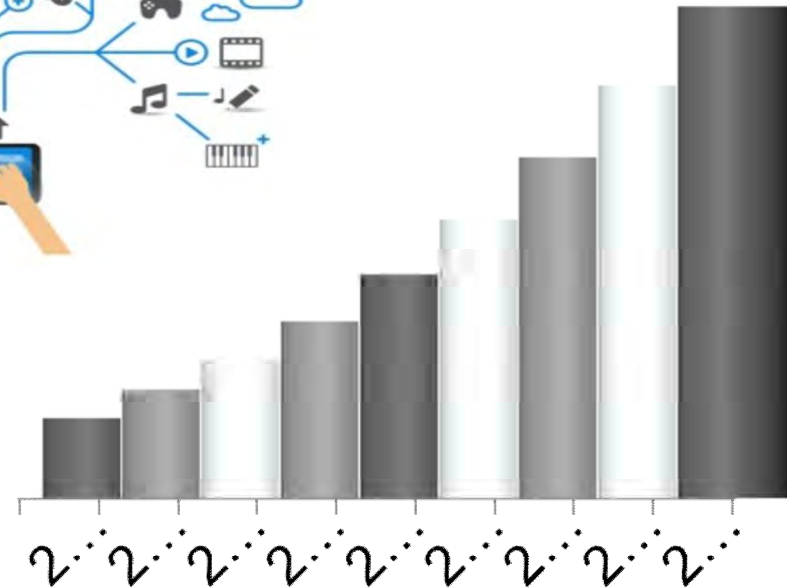
CYBER THREATS & EXPOSURES





PROLIFERATION OF CONNECTED DEVICES

2012	8.7 Billion
2013	11.2 Billion
2014	14.4 Billion
2015	18.2 Billion
2016	22.9 Billion
2017	28.4 Billion
2018	34.8 Billion
2019	42.1 Billion
2020	50.1 Billion



" The idea of having up to 50 Billion connected devices in the next few years is exciting. I also think it's scary. The scary part of it is the cyber security."

Ajay Banga,
President & Chief Executive, MasterCard Inc.

Jan 2017



CYBER THREAT IS GROWING

TOTAL NUMBER OF THREATS BLOCKED IN 2014

65,058,972,693

TOTAL NUMBER OF THREATS BLOCKED IN 2016

81,885,110,903



Source: Threats blocked by the Trend Micro Smart Protection Network in 2014 / 2016

COMMON CYBER THREATS



PHISHING / SPEAR PHISHING

- One click away from a cyber attack
- #1 delivery vehicle for malware is email attachments
- Spear phishing: Tailored email targeting a specific individual or group within an organization.
- Advanced Persistent Threat



RANSOMWARE

- Most profitable malware in 2016: USD 1Billion industry
- Crypto Ransomware - encryption used as a tool to hold critical data hostage.
- RaaS
- WannaCry



COMMON CYBER THREATS



DISTRIBUTED DENIAL OF SERVICE ATTACK

- Hacktivism
- Cyber Extortion: DDOs For Bitcoin
- IoT Botnets
- Mobile Phone Botnets

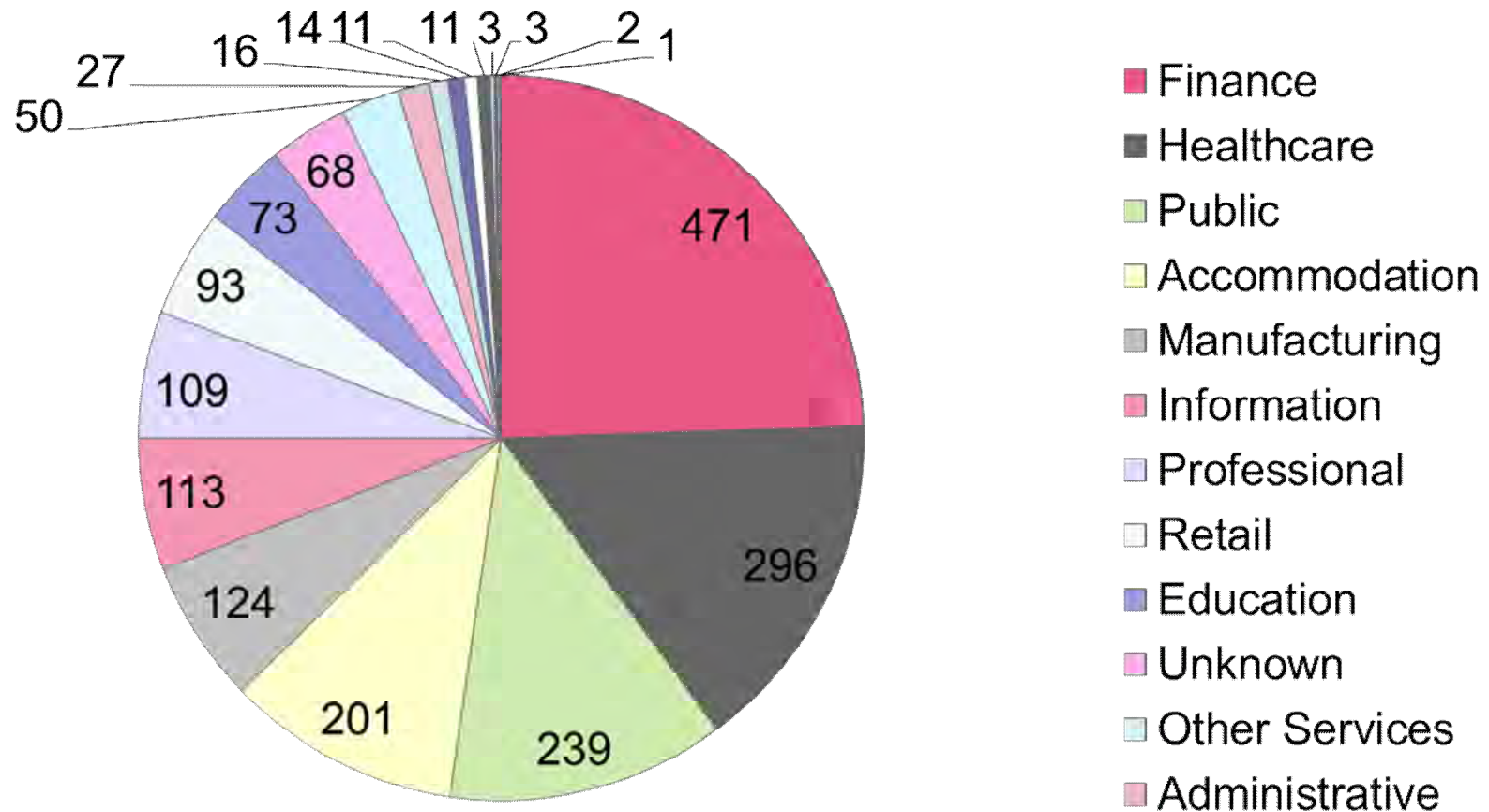


INJECTION

- Injection occurs when an attacker adds additional text to data that gets passed to an application, which then treats the additional data as a further instruction.
- Can lead to:
 - Direct access to data in database
 - Access to Database Management System
 - Access to Underlying Operating System

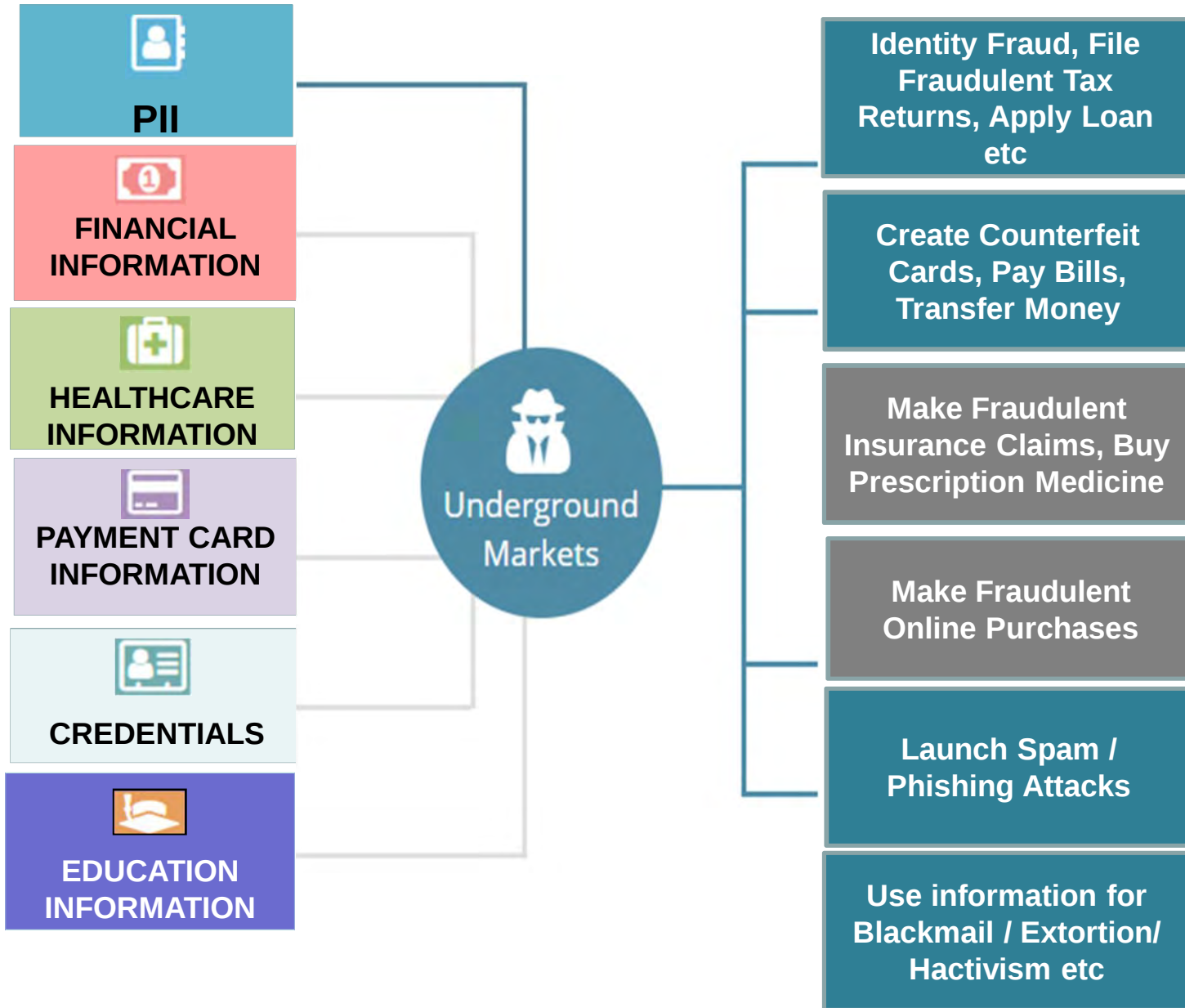


BROAD SPECTRUM OF INDUSTRIES AT RISK

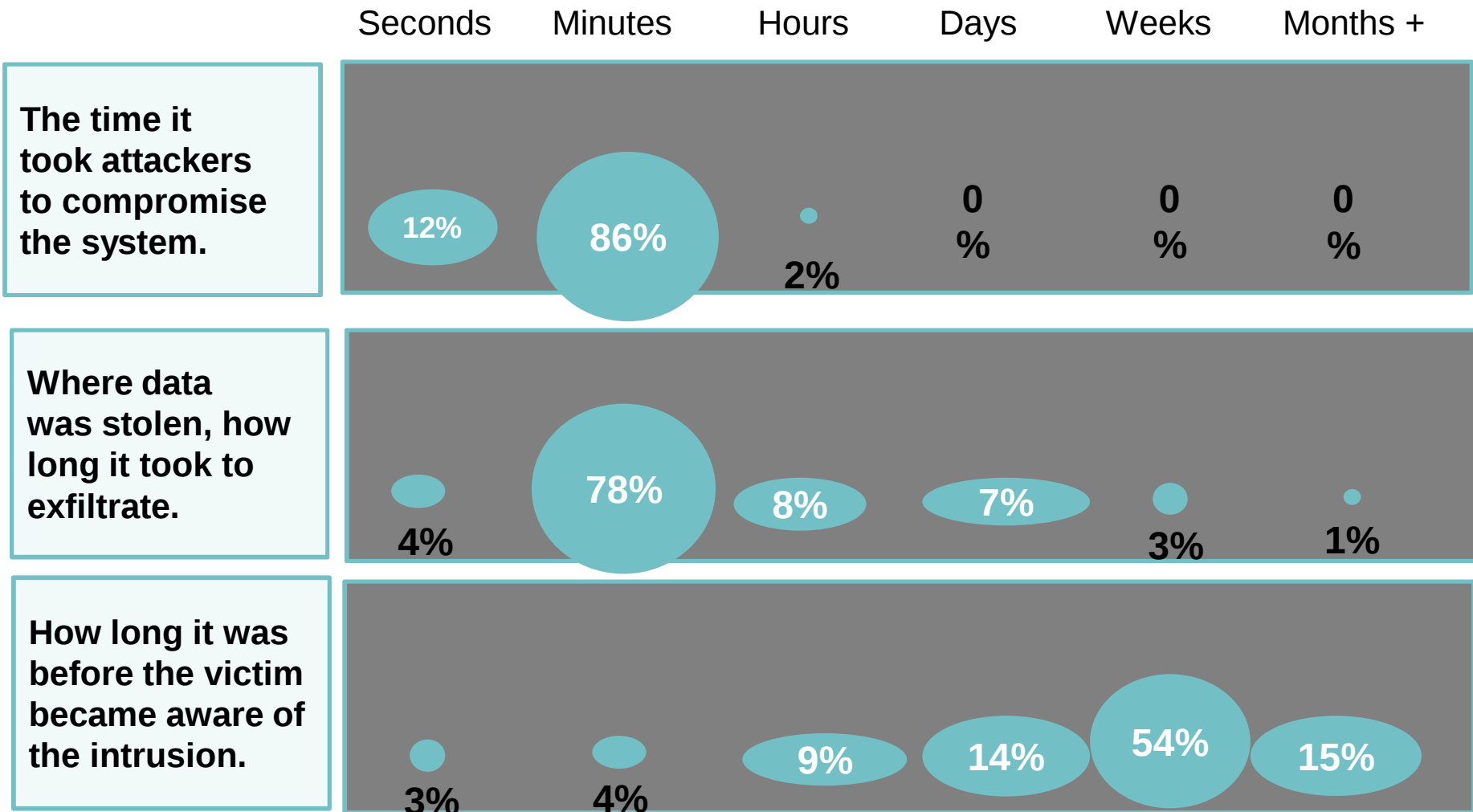


Source: Data from 2017 Verizon Data Breach Investigations Report. Numbers show breakdown of reported breaches by industry sector. Total number of reported breaches 1,935.

WHAT DO HACKERS DO WITH YOUR STOLEN IDENTITY ?

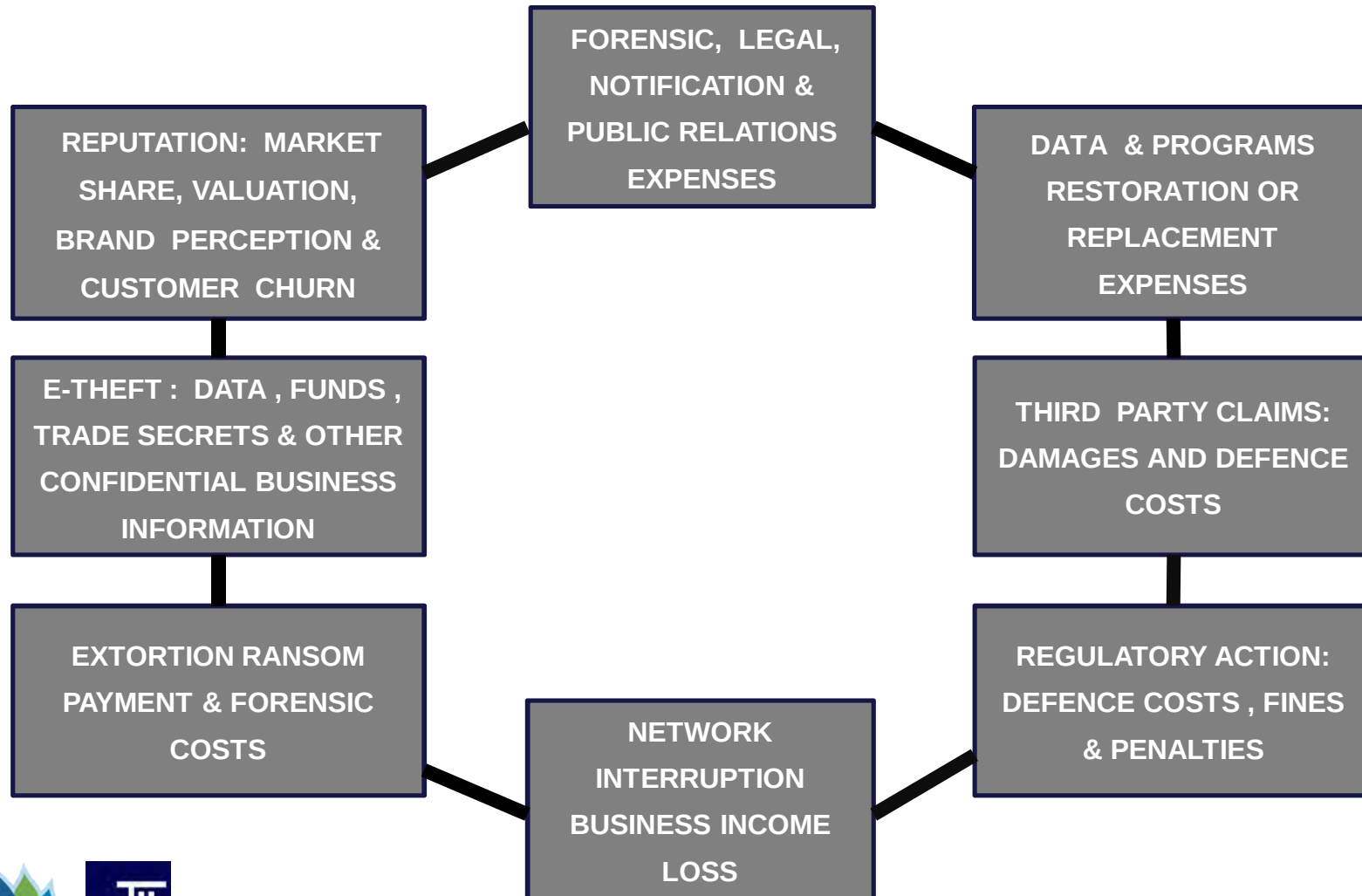


INCIDENT TIMELINE FOR FINANCIAL SERVICES



Source: 2016 Verizon Data Breach Investigation Report

NETWORK INTRUSION: FINANCIAL, LEGAL & REPUTATIONAL RISKS



US Financial Institutions DDOS attacks “were relentless, they were systematic, and they were widespread,”: U.S. Attorney General

“2012 Shamoon attack on Saudi Aramco was probably the most destructive cyber attack on a private business”: US Defence Secretary

Attack was “targeted and carefully planned”: Spore Ministry

“We had shut them out in April, but they found another backdoor,”: Yahoo Japan

“The threat is very persistent, adaptive and sophisticated – and it is here to stay”: SWIFT

We can, with great certainty, say that we have never experienced anything like this: A.P. Moller-Maesk

the “technical capabilities” of the attackers were evident

“In just half a day on Monday, Bank Indonesia detected 273 viruses and 67,000 spam emails to its email server and website “: Bank Official

“It was a race against time - more systems were corrupted with every passing minute. A longer delay might have prompted satellite distribution channels to seek reparation from, or, worse, contract cancellations with TV5Monde. We were saved from total destruction by the fact we had launched the channel that day and the technicians were there,” Director General, TV MONDE 5.



PART 3



PART 3

How ransomware works...

The following information is courtesy of CSM



Cyber-attacks...

...cost the global economy an estimated **\$445 billion** and were ranked the **most likely risk** by US leaders.

Source: *Global Risks Report 2016*. Image: REUTERS/Dado Ruvic



 Wana Decrypt0r 2.0



Ooops, your files have been encrypted!

Dutch

U heeft slechts 3 dagen om de betaling in te dienen. Daarna wordt de prijs verdubbeld. Ook als u niet over 7 dagen betaalt, kunt u uw bestanden voor altijd niet herstellen. We hebben gratis evenementen voor gebruikers die zo arm zijn dat ze niet in 6 maanden kunnen betalen.

Hoe betaal ik?

Betaling wordt alleen in Bitcoin geaccepteerd. Klik voor meer informatie op <About

Payment will be raised on
5/15/2017 16:27:35

Time Left
00:00:00:00

Your files will be lost on
5/19/2017 16:27:35

Time Left
01:05:15:35

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)
Picture by ThiceNL

 **bitcoin**
ACCEPTED HERE

Send \$600 worth of bitcoin to this address:

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Copy

Check Payment

Decrypt

 You have a new message:
I have already sent decryption keys to many customers who had sent me the correct amounts of bitcoin, and I guarantee the decryptions for such honest customers.

Send me a message with your unique bitcoin wallet address an hour before your payment.
Then you will receive the decryption key more quickly.

OK

bitcoins. Klik voor meer

s opgegeven.

ontroleren: 9:00 - 11:00 uur

bestanden decoderen.

act Us>.

en, en uw anti-virus al een

tijdje uit te schakelen, totdat u betaalt en de betaling wordt verwerkt. Als uw anti-virus automatisch wordt bijgewerkt en verwijderd, kan het uw bestanden niet herstellen, zelfs als u betaalt!



Cyber risk and risk management

The risks and opportunities which digital technologies, devices and media bring us are manifest. Cyber risk is never a matter purely for the IT team, although they clearly play a vital role. An organisation's risk management function need a thorough understanding of the constantly evolving risks as well as the practical tools and techniques available to address them.

What do we mean by cyber risk?

‘Cyber risk’ means any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems.

It will never happen to us....

All types and sizes of organisations are at risk, not only the financial services firms, defence organisations and high profile names which make the headlines.

[Cyber risk - The Institute of Risk Management](https://www.theirm.org/knowledge-and-resources/thought.../cyber-risk/)

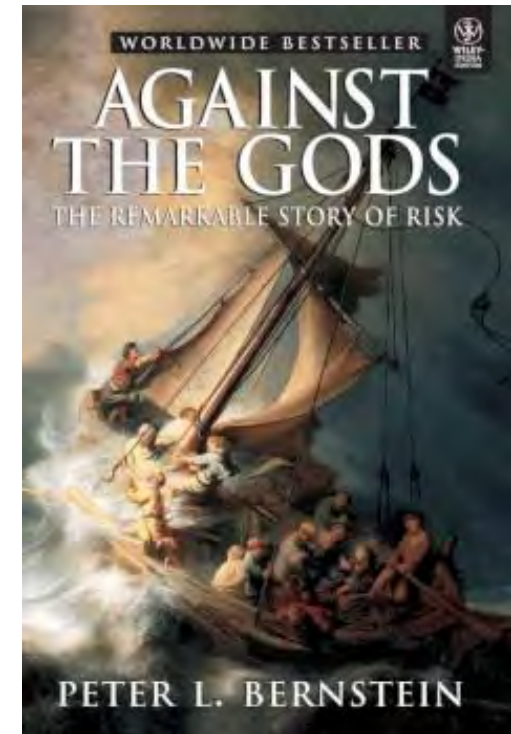
<https://www.theirm.org/knowledge-and-resources/thought.../cyber-risk/>



The revolutionary idea that defines the boundary between modern times and the past is the mastery of risk: the notion that the future is more than a **whim of the gods** and that men and women **are not passive before nature**.

Until human beings discovered a way across that boundary, the future was the mirror of the past or the murky domain of oracles and soothsayers who held a monopoly over knowledge of anticipated events.

Peter Bernstein, *Against the Gods: The Remarkable Story of Risk*





TECH

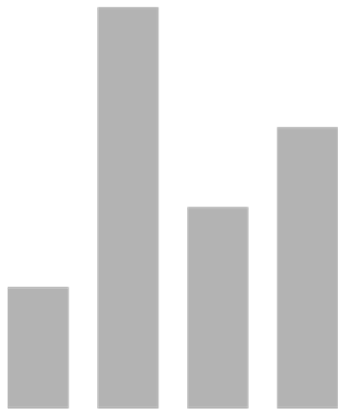
Russia's Top Religious Official Sprays Holy Water on Computers to Fend Off Ransomware Virus

BY IAN M. CHEONG
15 MAY 2017



<https://heatst.com/tech/russias-secret-weapon-against-ransomware-virus-holy-water/>

Recent poll on ransomware in the UK



44% of businesses infected

60% had backups

65% paid the ransom

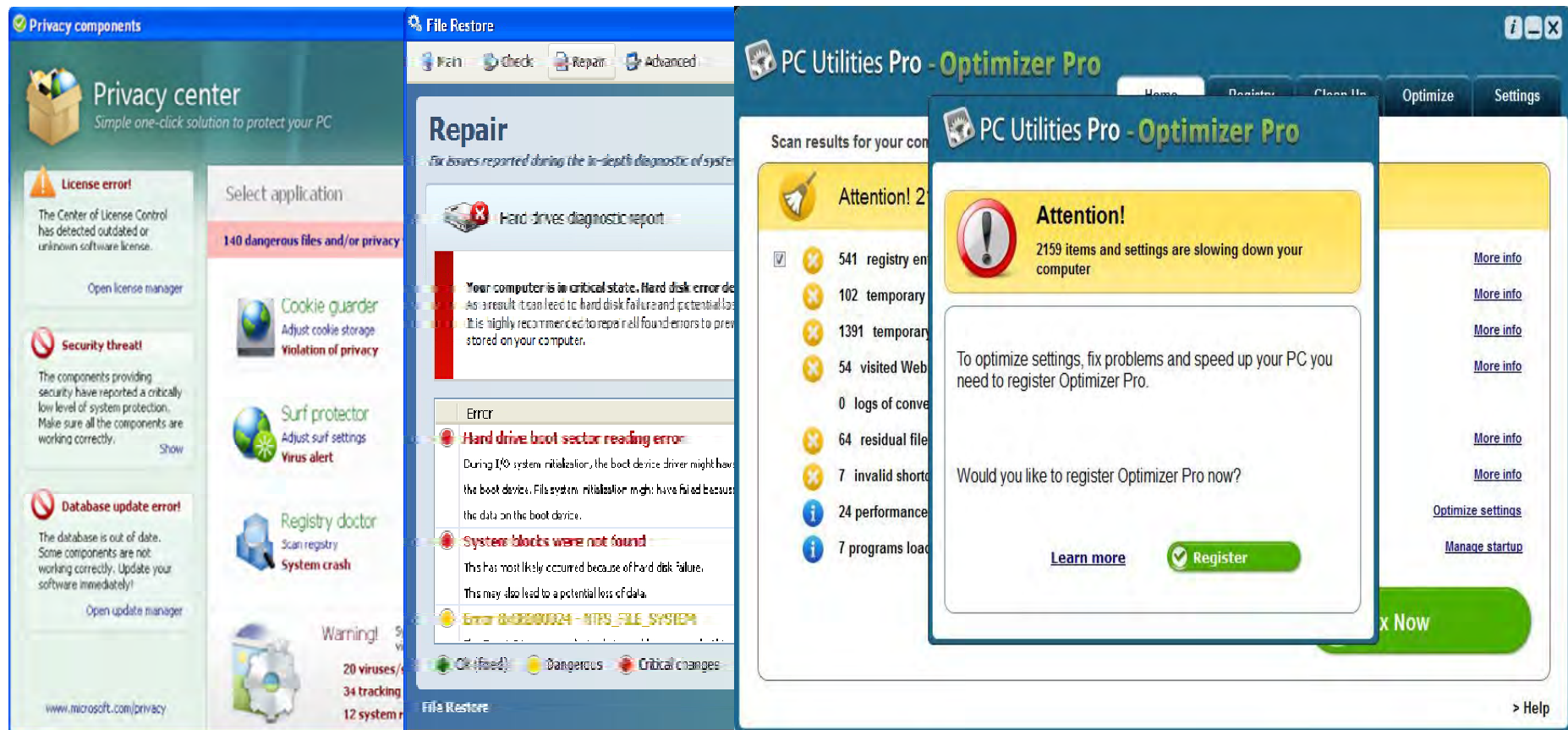
Average ransom sum £540

Loss of business productivity comes on top, exceeding ransom

Ransomware Evolution



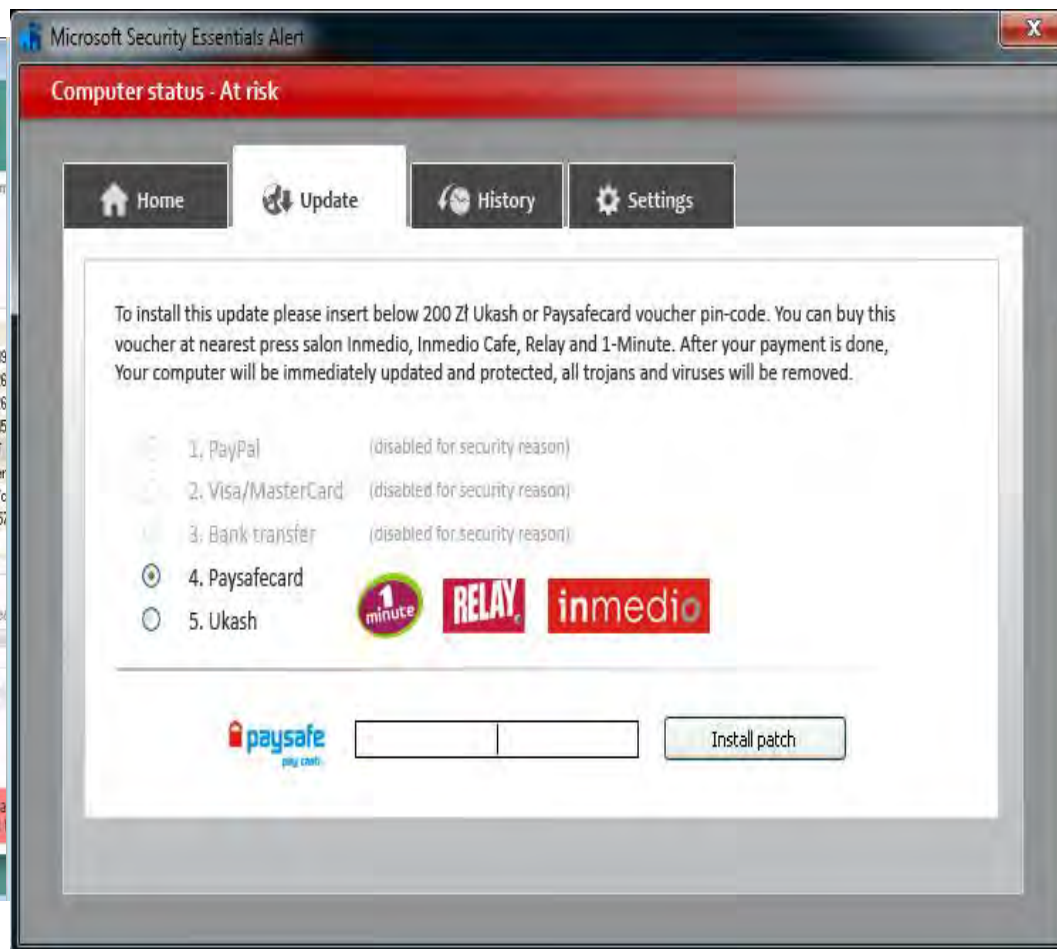
Misleading Applications



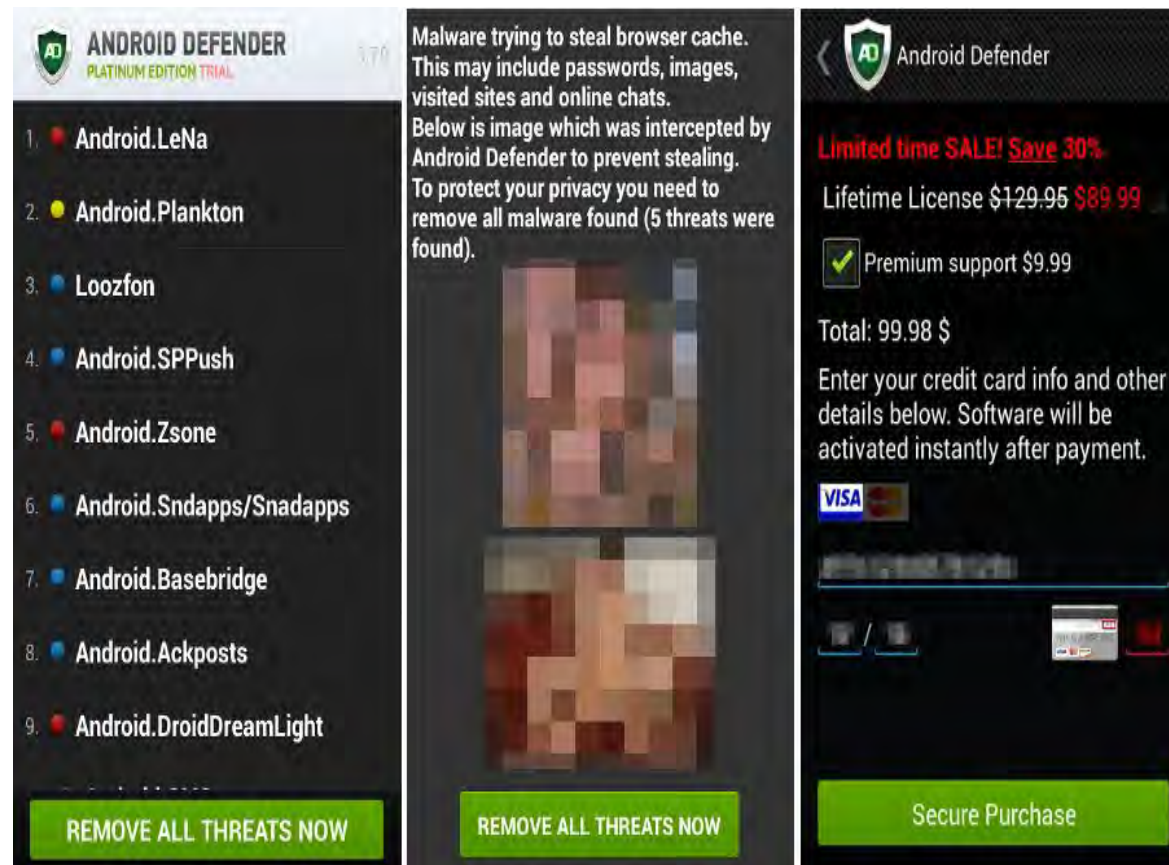
Rogue/Fake Antivirus



Rogue/Fake Antivirus



Rogue/Fake Antivirus (Android)



(Browser) Locker Ransomware

The image displays two examples of browser ransomware lockers. The left screenshot shows a page from 'ruteenagers.com' with a header for the 'INTERPOL ASSOCIATION NATIONAL SECURITY AGENCY'. It displays the IP address 198.23.71.112 and accuses the user of viewing or disseminating banned pornography. It demands a payment of 300 via MoneyPak to unlock the browser. The right screenshot shows a page from 'block.zeropoliceint1.biz' with a header for the 'Bundesamt für Sicherheit in der Informationstechnik' and 'BUNDESPOLIZEI GvU'. It displays the IP address 92.231.76.168 and accuses the user of accessing the browser from Germany. It demands a payment of 100 via PaysafeCard to unlock the browser. Both pages include detailed instructions on how to make the payment and warnings about legal consequences.

Left Ransomware (ruteenagers.com):

- IP: 198.23.71.112
- Country: United States
- Region: California
- City: ---
- Your Location: 34.0522, -118.2437
- Operating System: Windows
- Remaining time: 48:00:00
- Payment: 300 via MoneyPak
- Accusation: You are accused of viewing/storage and/or dissemination of banned pornography (child pornography/zoophilia/rape etc.). You have violated World Declaration on non-proliferation of child pornography. You are accused of committing the crime envisaged by Article 161 of United States of America criminal law.
- Warning: Your browser has been blocked up for safety reasons listed below. All the actions performed on this PC are fixed. All your files are encrypted. AUDIO AND VIDEO RECORDING IN PROGRESS.
- Instructions: How do I unlock the browser using the MoneyPak? 1. Find a retail location (7 Eleven, Wal-Mart, Walgreens, Rite Aid Pharmacy, Kmart, CVS Pharmacy, Kroger, Dollar General, Family Dollar, InComm, Kumbon, Coinstar-EPS) near you. 2. Look for a MoneyPak in the prepaid section. Take it to the cashier and load it with cash. 3. To pay fine you should enter the digits MoneyPak resulting pass in the payment form and press "Settle MoneyPak".

Right Ransomware (block.zeropoliceint1.biz):

- IP: 92.231.76.168
- Land: Germany
- Bereich: 01
- Stadt: Karlsruhe
- Payment: 100 via PaysafeCard
- Accusation: Ihnen wird die Ansicht/Lagerung und/oder den Vertrieb von pornographischem Material von verbotenen Inhalten (Kinderpornografie/Zoophilie/Vergewaltigung, etc.) vorgeworfen. Sie haben die Allgemeine Erklärung zur Bekämpfung der Verbreitung von Kinderpornographie verletzt wegen einer Straftat nach Artikel 161 des Strafgesetzbuches der Bundesrepublik Deutschland.
- Warning: WARNUNG! Zugang von Ihrem Browser wurde vorläufig aus den unten aufgelisteten Gründen gesperrt. Alle Aktivitäten des Computers aufgezeichnet wurden. Alle Ihre Dateien werden verschlüsselt.
- Instructions: Artikel 161 des Strafgesetzbuches der Bundesrepublik Deutschland sieht eine Freiheitsstrafe von 5 bis 11 Jahren in solchen Fällen vor.



Locker Ransomware



METROPOLITAN POLICE

ATTENTION! ILLEGAL ACTIVITY WAS REVEALED!

Your operational system is locked as a result of Great Britain law violation!

The following violations were revealed: your IP address was detected on illegal pornographic sites including child pornography, zoophilia and violent scenes with children. Pornographic video with elements of violence and child pornography were revealed on your PC!

Illegal SPAM or harmful program is also found on your PC!

The lock is designed to minimize possible distribution of the above materials from your PC in the internet!

Your personal data: IP: Browser: Internet Explorer 6.0 OS: Windows XP Country: City: RUS

For your PC to be unlocked you have to pay penalty equal to 1000! The penalty will be paid during 24 hours from the moment when your PC was locked. After penalty is not paid all the data will be removed from your PC!

There are 2 ways of payment:

- 1) You can buy the Ukash coupon for the amount of 1000. Enter the Ukash coupon number in payment field and press OK or send the coupon number by email: metropoliTan@vodafone.com You can buy the Ukash coupon at any available point.
- 2) You can pay the penalty by means of Paysafecard. Payment by means of Paysafecard is to be effected by the amount of 1000. Enter the pin code from back of Paysafecard and press OK or send the pin code by email: metropoliTan@vodafone.com

You can buy Paysafecard at any available point. As soon as payment is effected your PC will be unlocked during 24 hours from the moment of payment.

At night we observed (C.I. 121)

Logos: Kaspersky, bitdefender, AVIRA, symantec, AntiVirus, Panda.



PCEU Police Central e-crime Unit
Specialist Crime Directorate
Police Central e-crime Unit

To unlock your computer and to avoid other legal consequences, you are obligated to pay a fine.

All activity of this computer has been recorded
If you use a webcam, videos and pictures were saved for identification

Video-recording: ON

You can be clearly identified by resolving your IP address and the associated hostname

Your IP Address: [redacted]
Your Hostname: **British Telecommunications**
Location: **United Kingdom**

Your Computer has been locked!

The work of your computer has been suspended on the grounds of unauthorized cyberactivity.

Described below are possible violations, you have made:

- Article 274 – Copyright**
A fine or imprisonment for the term of up to 4 years (The use or sharing of copyrighted files – movies, software)
- Article 183 – Pornography**
A fine or imprisonment for the term of up to 2 years (The use or distribution of pornographic files)
- Article 184 – Pornography involving children (under 18 years)**
Imprisonment for the term of up to 15 years (The use or distribution of pornographic files)
- Article 104 – Promoting Terrorism**
Imprisonment for the term of up to 25 years (You have visited websites of terrorist organizations)
- Article 297 – Neglect computer use, entailing serious consequences**
A fine or imprisonment for the term of up to 2 years

1. [Image of cash] 2. [Image of a card reader] 3. [Image of a laptop screen showing a payment page]

Ukash You can get Ukash from hundreds of thousands of global locations, online, from wallets, from kiosks and ATMs.

Exchange your cash for a Ukash voucher and use your voucher code in form below.

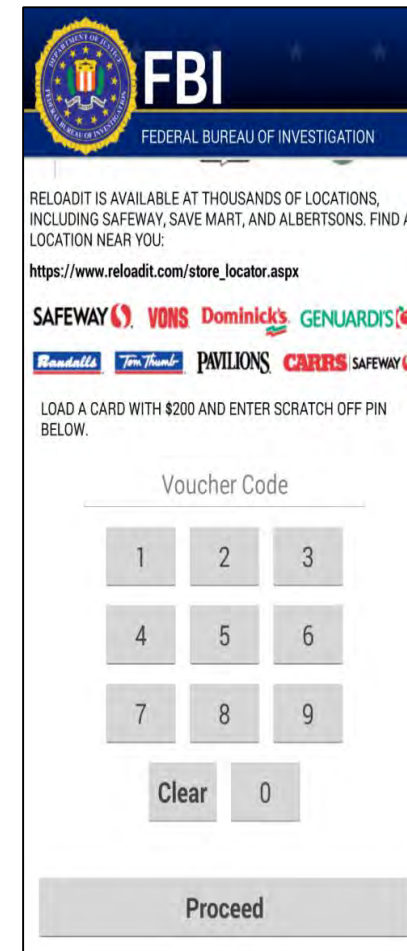
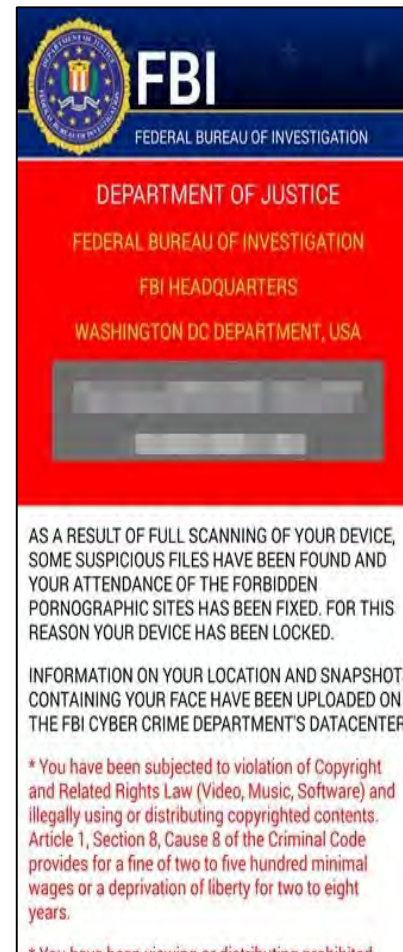
Code: [1][2][3][4][5][6][7][8][9][0] **Submit**

paysafecard Paysafecard is available from 450,000 sales outlets worldwide, in the United Kingdom, exclusively from all PayPoint outlets.

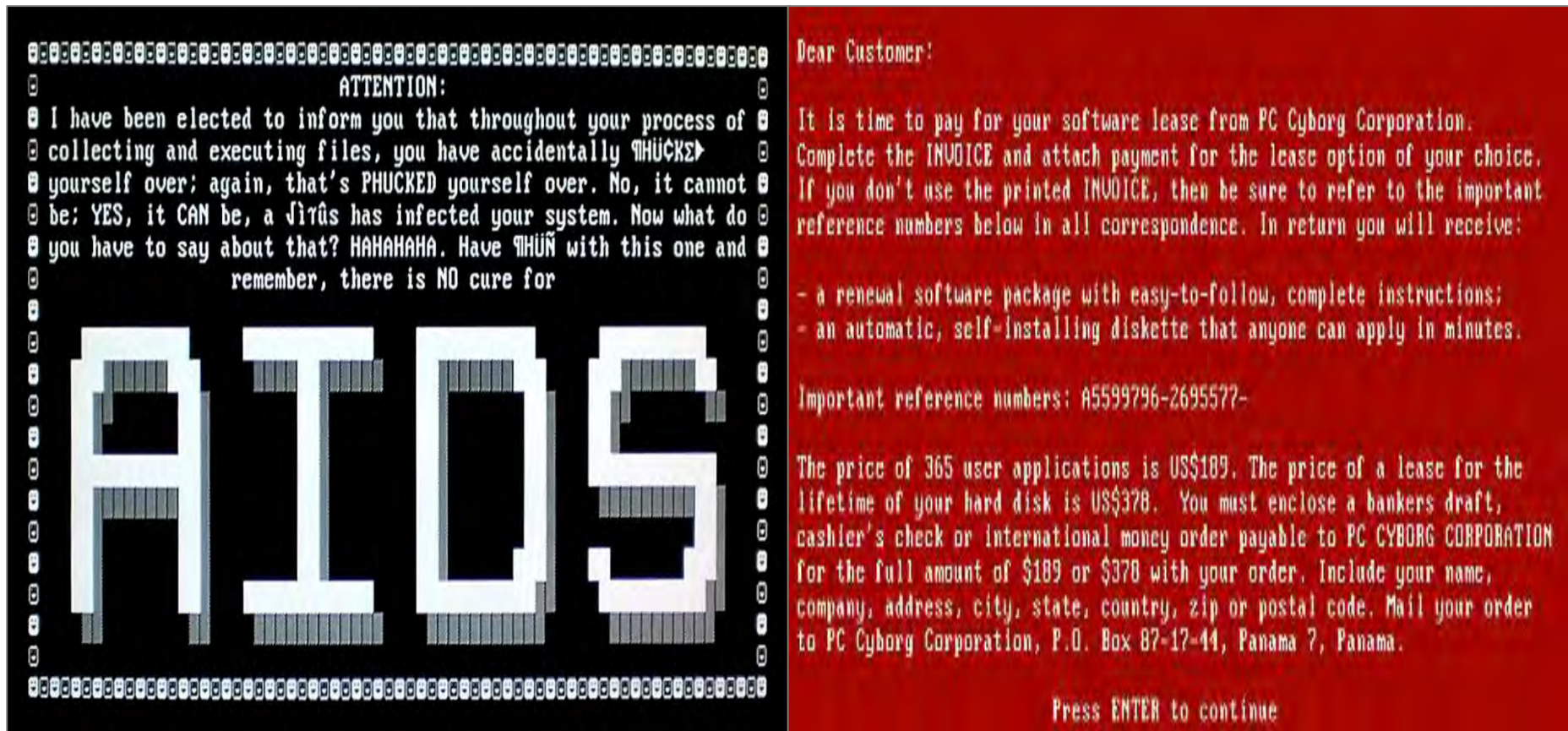
Exchange your cash for a Paysafecard voucher and use your voucher code in form below.



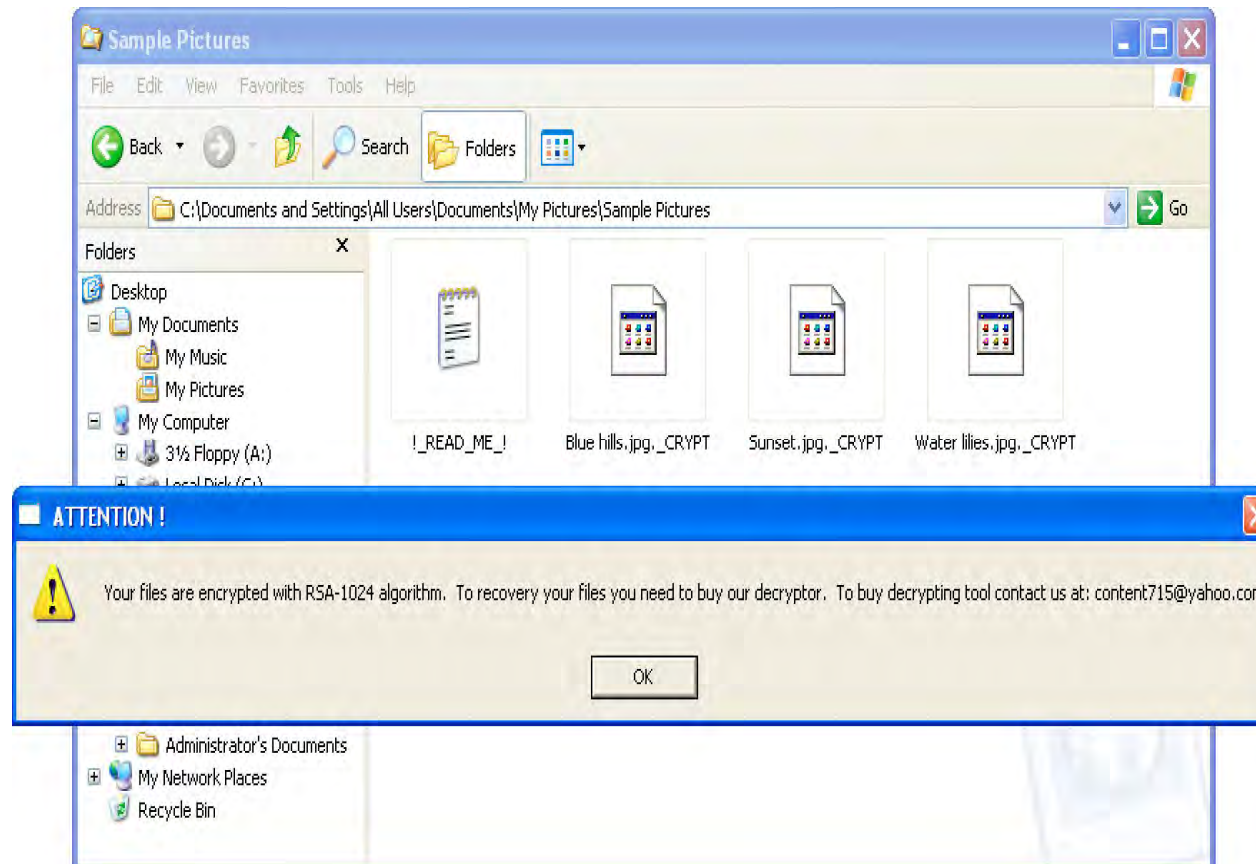
Locker Ransomware (Android)



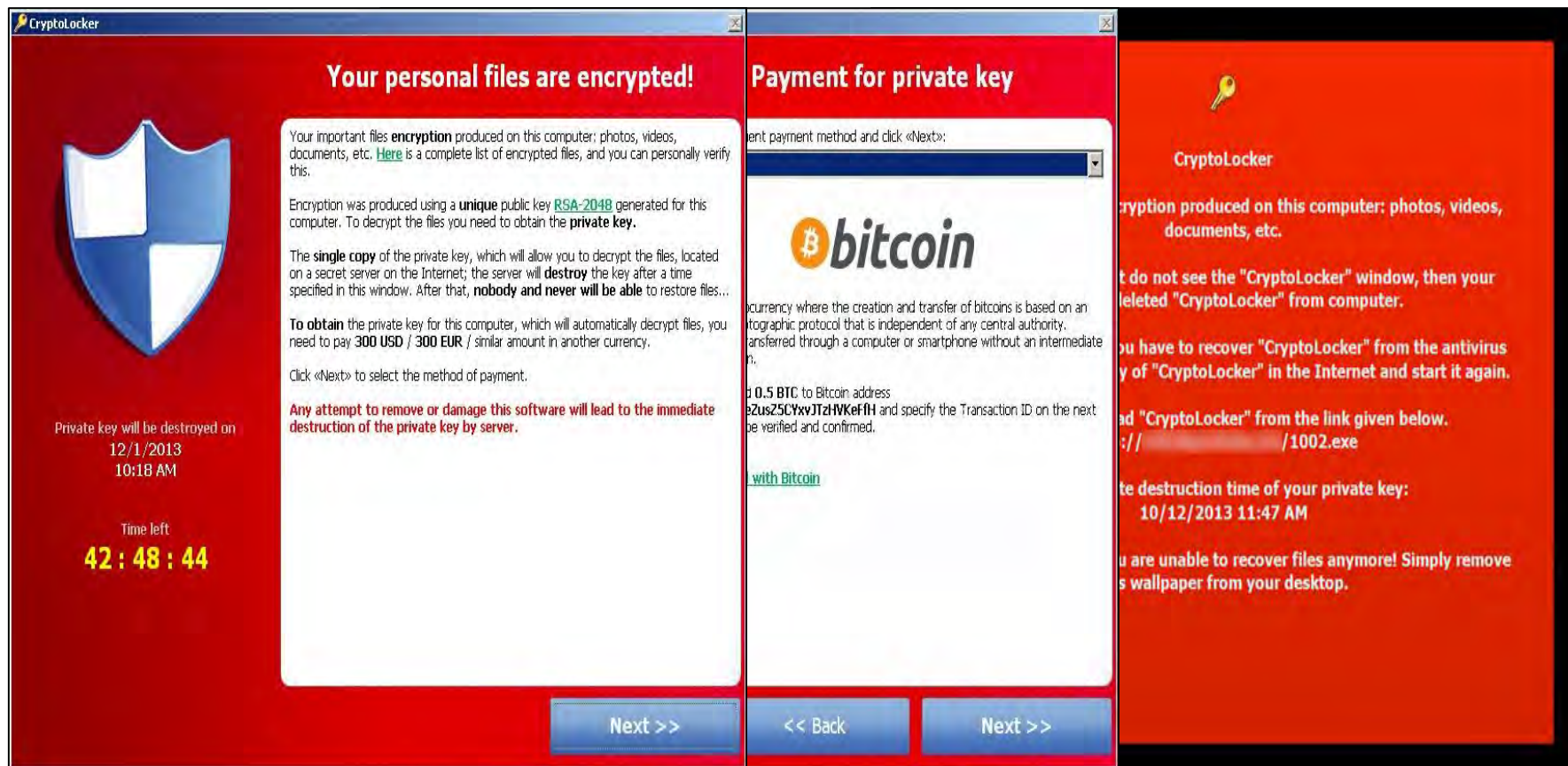
Ransomware (AIDS / PC Cyborg) (1989)



Crypto-Ransomware (Gpcode) (2005)



Crypto-Ransomware (Cryptolocker) (2013)



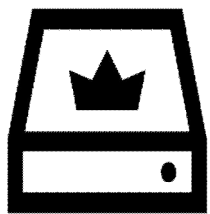
200 Crypto-Ransomware Families

.CryptoHasYou., 777, 7ev3n, 7h9r, 8lock8, **Alfa Ransomware**, **Alma Ransomware**, Alpha Ransomware, AMBA, Apocalypse, ApocalypseVM, AutoLocky, BadBlock, BaksoCrypt, Bandarchor, Bart, BitCryptor, BitStak, BlackShades Crypter, Blocatto, Booyah, Brazilian, BrLock, Browlock, Buchi, BuyUnlockCode, Cerber, Chimera, CoinVault, Covertion, Cryaki, Crybola, CryFile, CryLocker, **CrypMIC**, Crypren, Crypt38, Cryptear, **CryptFile2**, CryptInfinite, CryptoBit, CryptoDefense, CryptoFinancial, CryptoFortress, CryptoGraphic Locker, CryptoHost, CryptoJoker, **CryptoLocker**, Cryptolocker 2.0, CryptoMix, CryptoRoger, CryptoShocker, CryptoTorLocker2015, CryptoWall 1, CryptoWall 2, CryptoWall 3, CryptoWall 4, CryptXXX, CryptXXX 2.0, CryptXXX 3.0, **CryptXXX 3.1**, CTB-Faker, **CTB-Locker**, CTB-Locker WEB, CuteRansomware, DeCrypt Protect, DEDCryptor, DetoxCrypto, DirtyDecrypt, DMALocker, DMALocker 3.0, Domino, EDA2 / HiddenTear, EduCrypt, El-Polocker, Enigma, FairWare, Fakben, Fantom, Fonco, Fsociety, Fury, GhostCrypt, Globe, GNL Locker, Gomasom, Goopic, Gopher, Harasom, Herbst, Hi Buddy!, Hitler, HolyCrypt, HydraCrypt, iLock, iLockLight, International Police Association, JagerDecryptor, Jeiphoos, Jigsaw, Job Crypter, **KeRanger**, KeyBTC, KEYHolder, KimcilWare, Korean, Kozy.Jozy, KratosCrypt, KryptoLocker, LeChiffre, Linux.Encoder, Locker, **Locky**, Lortok, LowLevel04, Mabouia, Magic, MaktubLocker, MIRCOP, MireWare, Mischa, MM Locker, Mobef, NanoLocker, Nemucod, NoobCrypt, Nullbyte, ODCODC, Offline ransomware, OMG! Ransomware, Operation Global III, PadCrypt, Pclock, **Petya**, PizzaCrypts, PokemonGO, PowerWare, PowerWorm, PRISM, R980, RAA encryptor, Radamant, Rakhni., Rannoh, Ransom32, RansomLock, Rector, RektLocker, RemindMe, Rokku, Samas-Samsam, Sanction, Satana, Scraper, Serpico, Shark, ShinoLocker, Shujin, Simple_Encoder, SkidLocker / Pompous, Smr32, SNSLocker, Sport, Stampado, Strictor, Surprise, SynoLocker, SZFLocker, TeslaCrypt 0.x - 2.2.0, TeslaCrypt 3.0+, TeslaCrypt 4.1A, TeslaCrypt 4.2, Threat Finder, **TorrentLocker**, TowerWeb, Toxcrypt, Troldesh, TrueCrypter, Turkish Ransom, UmbreCrypt, Ungluk, Unlock92, VaultCrypt, VenusLocker, Virlock, Virus-Encoder, WildFire Locker, Xorist, XRTN, Zcrypt, **Zepto**, Zimbra, Zlader / Russian, Zyklon.....

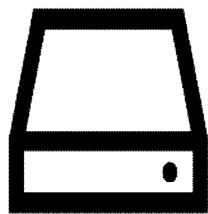
.....Wannacry....Notpetya.....



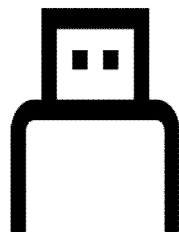
Crypto-Ransomware (Targets)



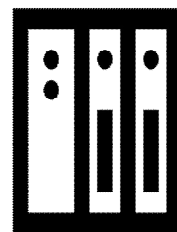
OS Disk



Local Disk(s)



**Connected
Device(s)
(USB)**
(e.g. Backup Disk)



**Mapped Network
Drive(s)**
(e.g. NAS / File
Servers)



**Other Accessible
Folders / Shared
Local Network**
(e.g. NAS / File
Servers)



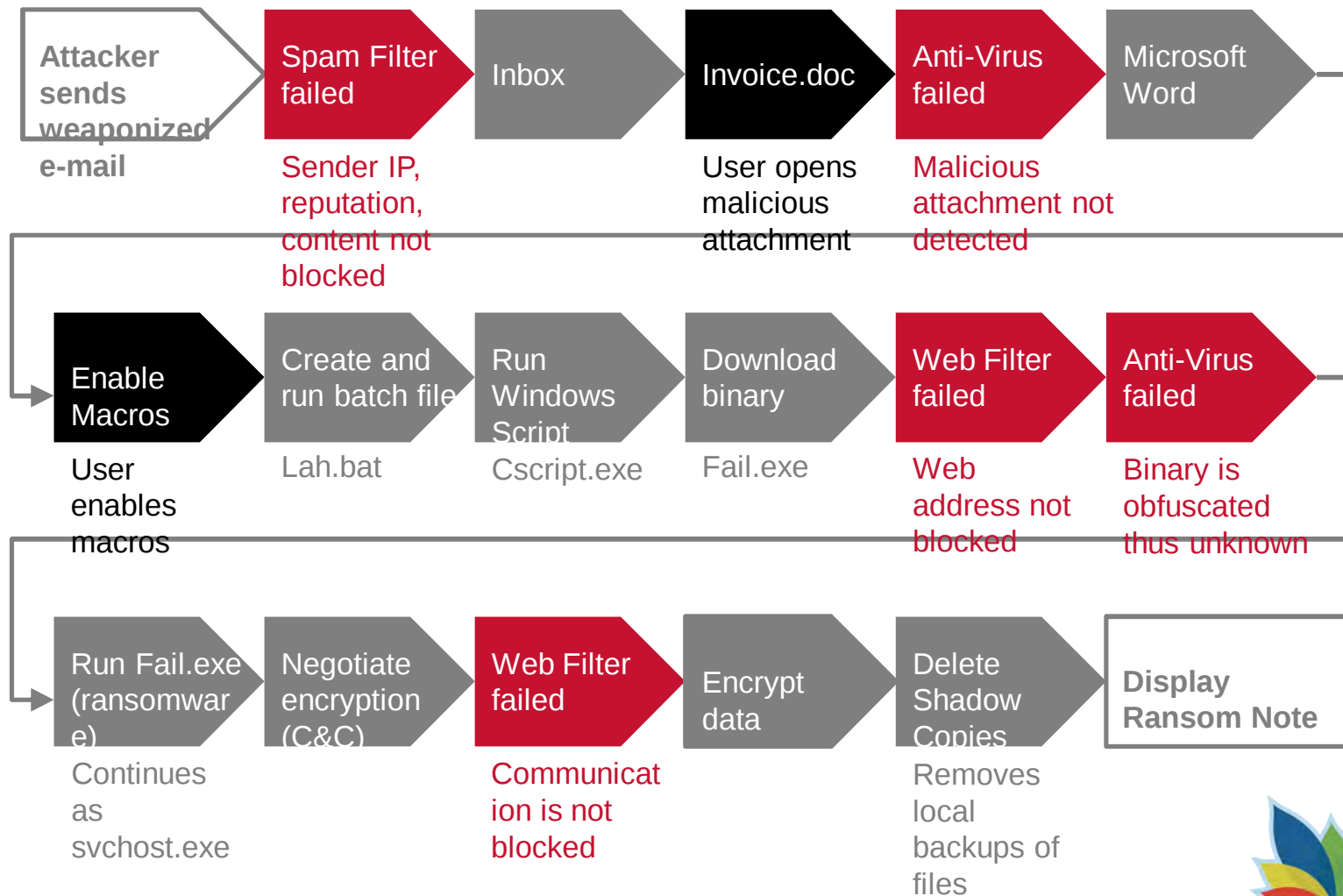
Dropbox



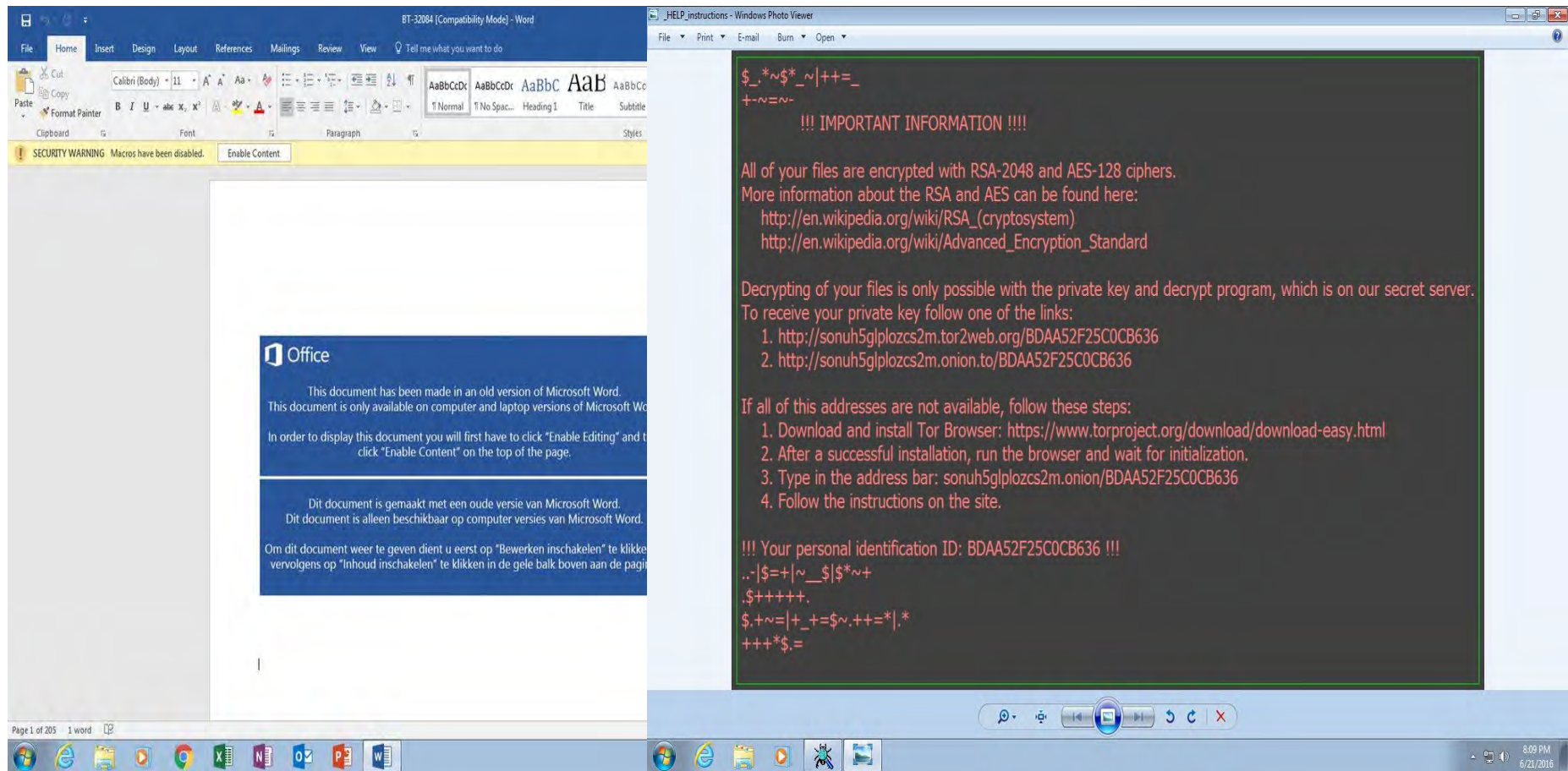
OneDrive



Social Engineering Flow (Locky ransomware, .doc)



Social Engineering Flow (Locky ransomware, .docm)



Security Overview – State of the Nation

Today's approach to IT Security is Falling Behind....

**Attack surface exponentially larger –
lowest hanging fruit**

Laptops/Desktops

Phones/Tablets

Virtual servers/desktops

Cloud servers/storage

Threats more sophisticated

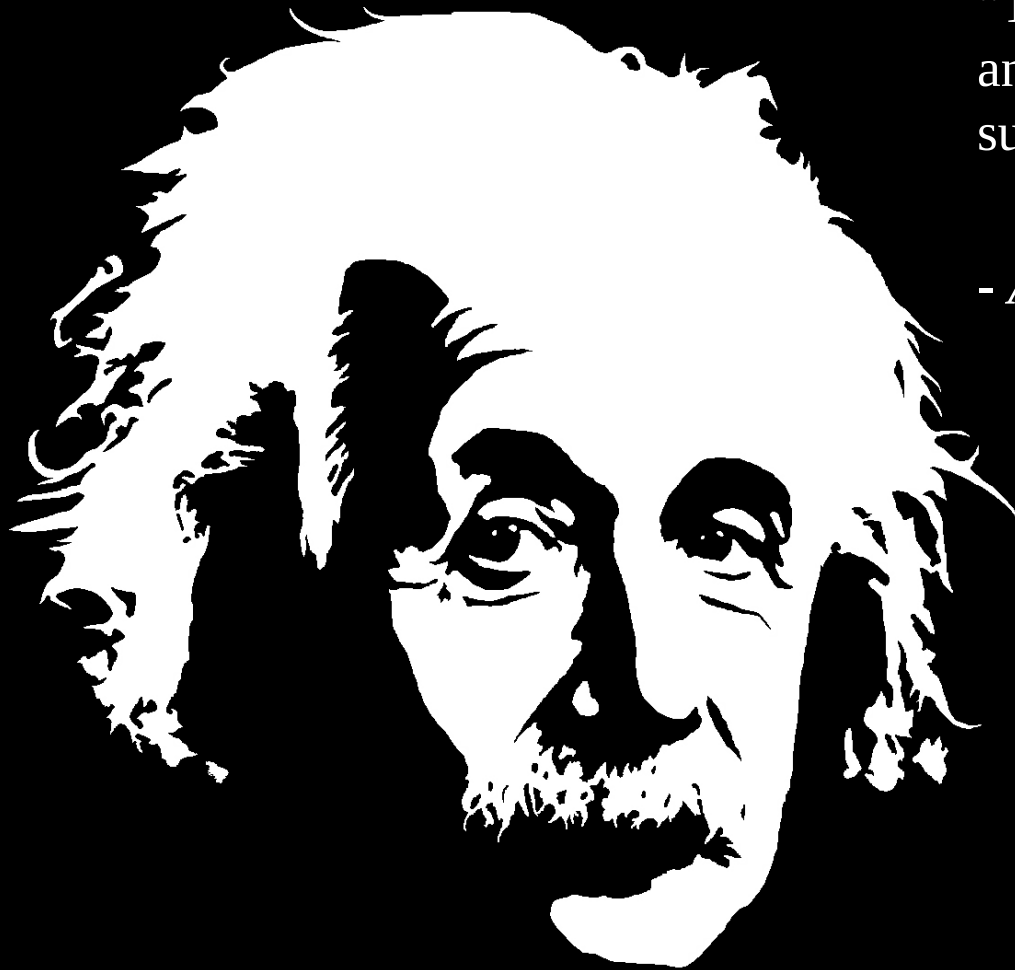
Attacks are more coordinated than
defenses

Volume and sophistication

Vanishing security perimeters

The rise of BYOD and personal Cloud
storage are eroding the network perimeter



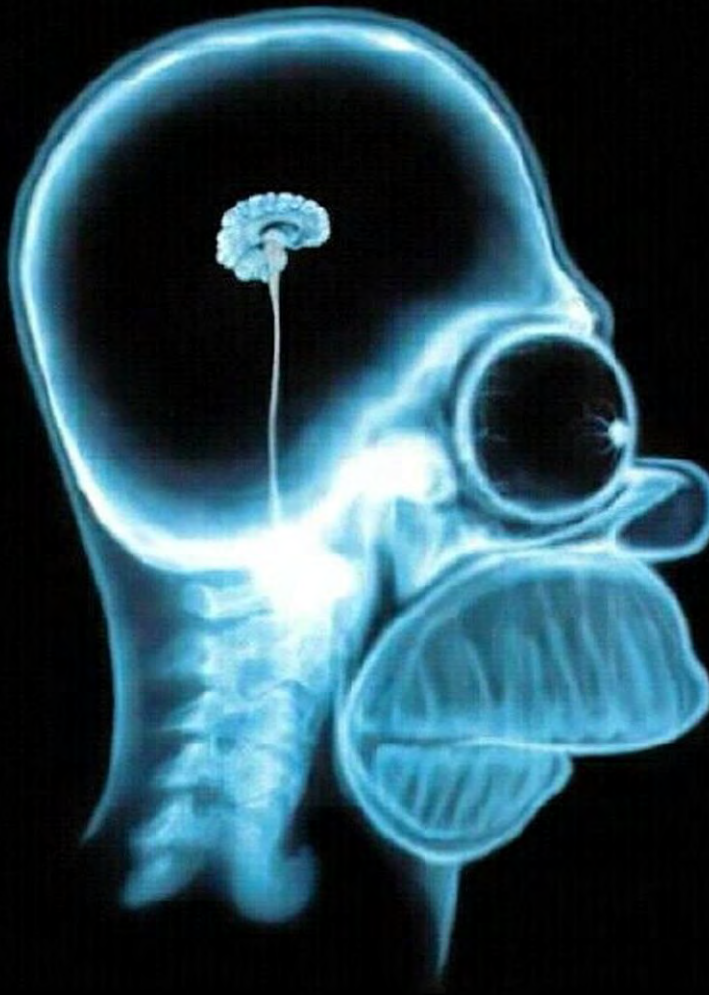


“Two things are infinite: The universe and human stupidity, and I’m not so sure about the former.”

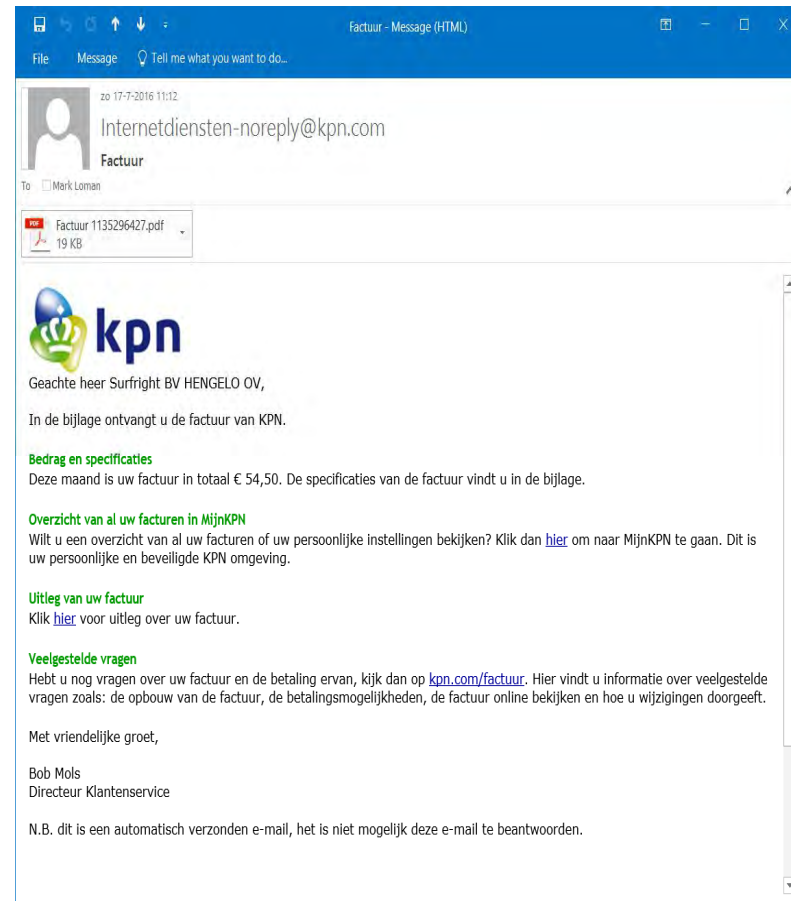
- *Albert Einstein*



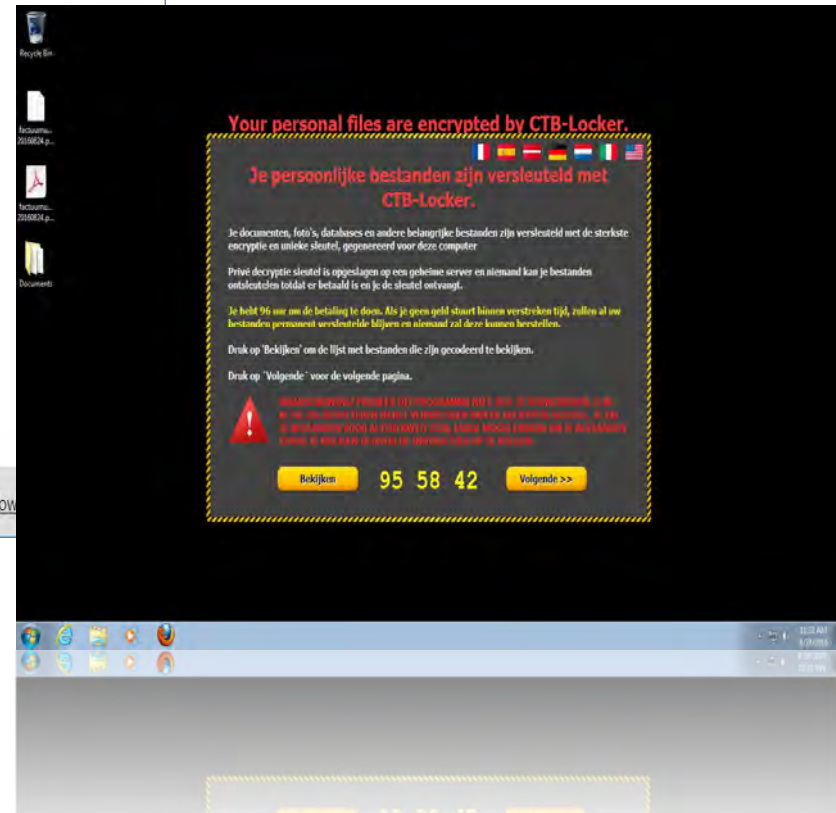
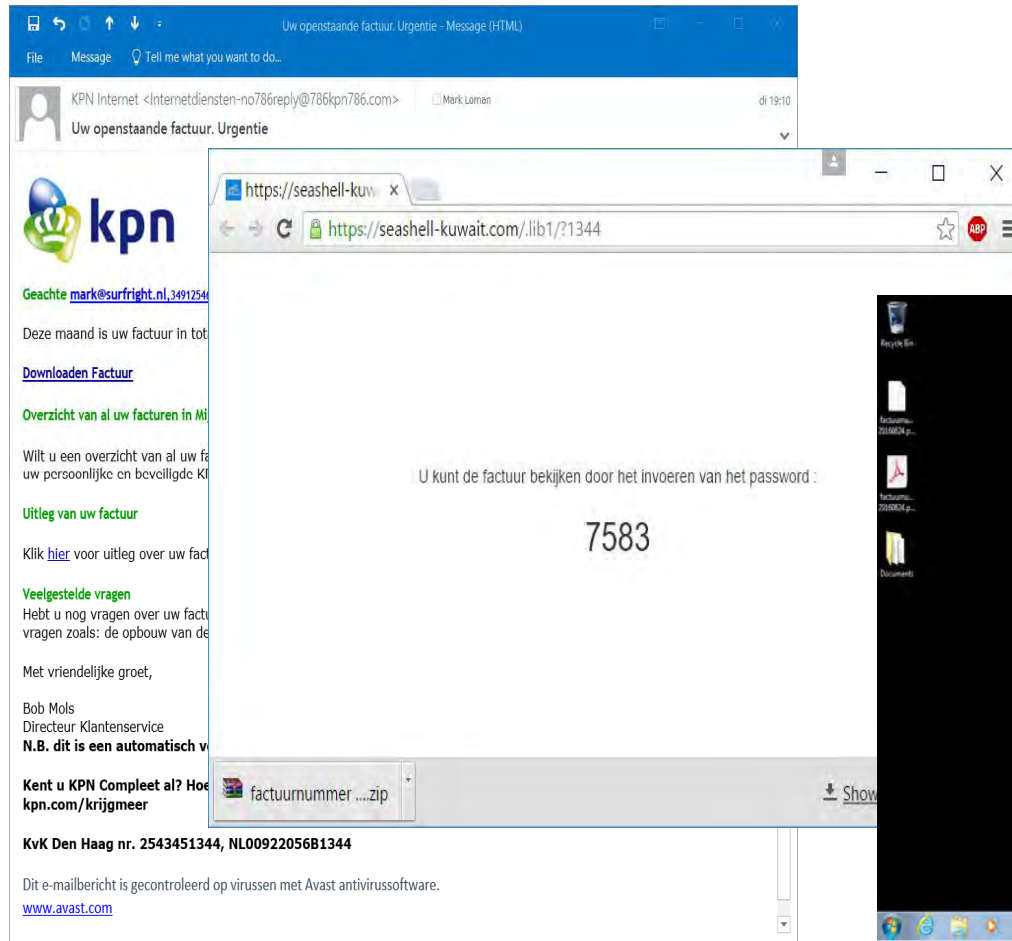
What is social engineering?



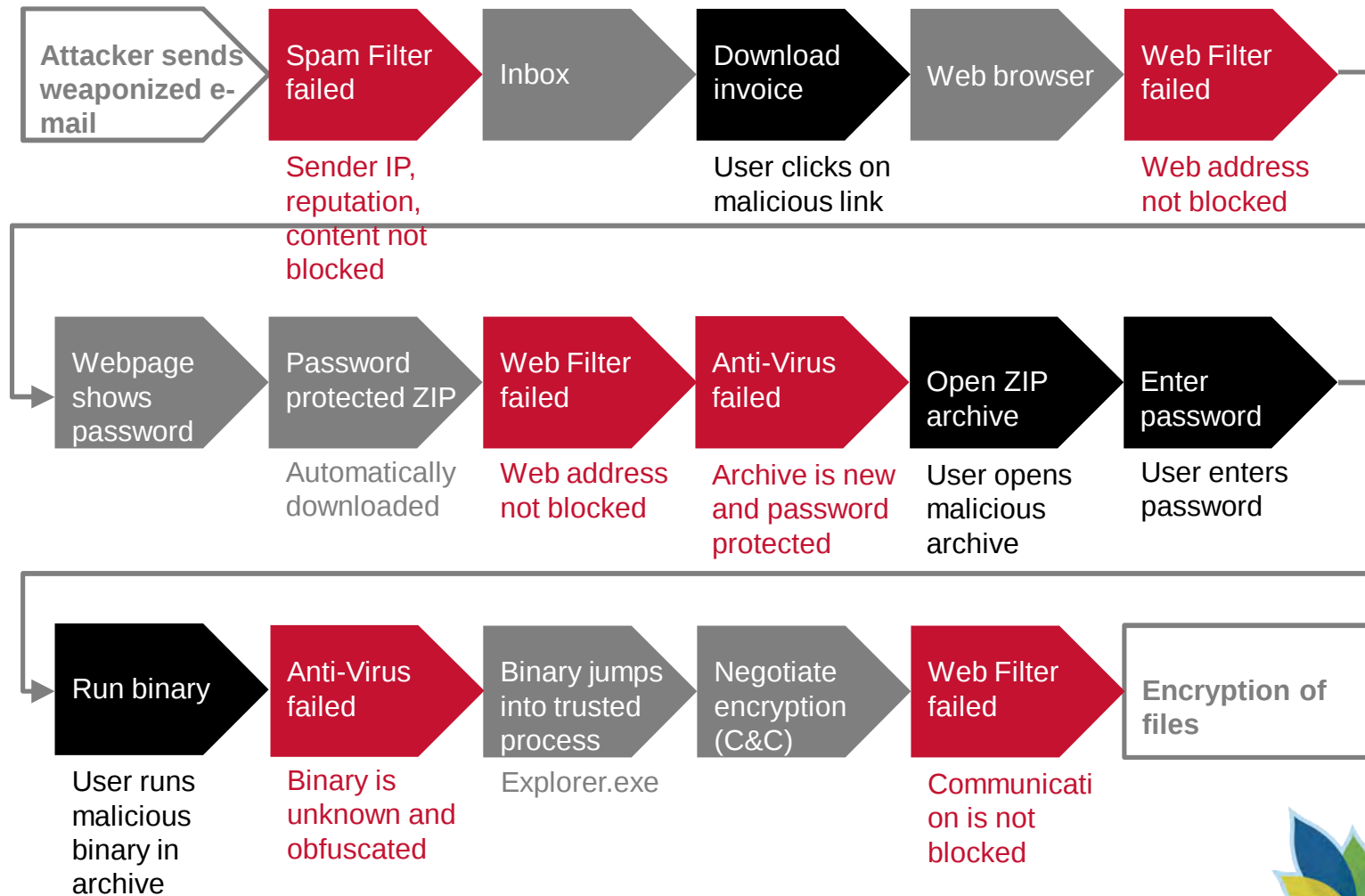
Social Engineering Example



Social Engineering Example



Social Engineering Flow (CTB-Locker ransomware)



Why email?

SPAM

Spray and pray

Campaigns generally cheap relatively unsophisticated means of delivering malware.

Renting time on a spam botnet is inexpensive and social engineering must be used.

Approach is remarkably effective, especially when the email lures are carefully crafted.

benefit that a fully-patched machine can still be infected.

Social Engineering

Malicious e-mail attachment:

Executable in archive (e.g. invoice.zip)

Executable in password protected archive

Executable with double extension (e.g. invoice.pdf.exe in invoice.zip)

Microsoft Office document with malicious VBA macro (.doc, .docm, .xls, .pub) dropping .EXE

Windows Script in archive (e.g. invoice.JS) dropping .EXE, .DLL



Comparison: Spam vs Exploit Kits

Angler revenue in a day



90,000 victims

9,000 served exploits

40% success rate

62% of infections
delivered Ransomware



Understanding vulnerabilities

Flaws

Features

User error

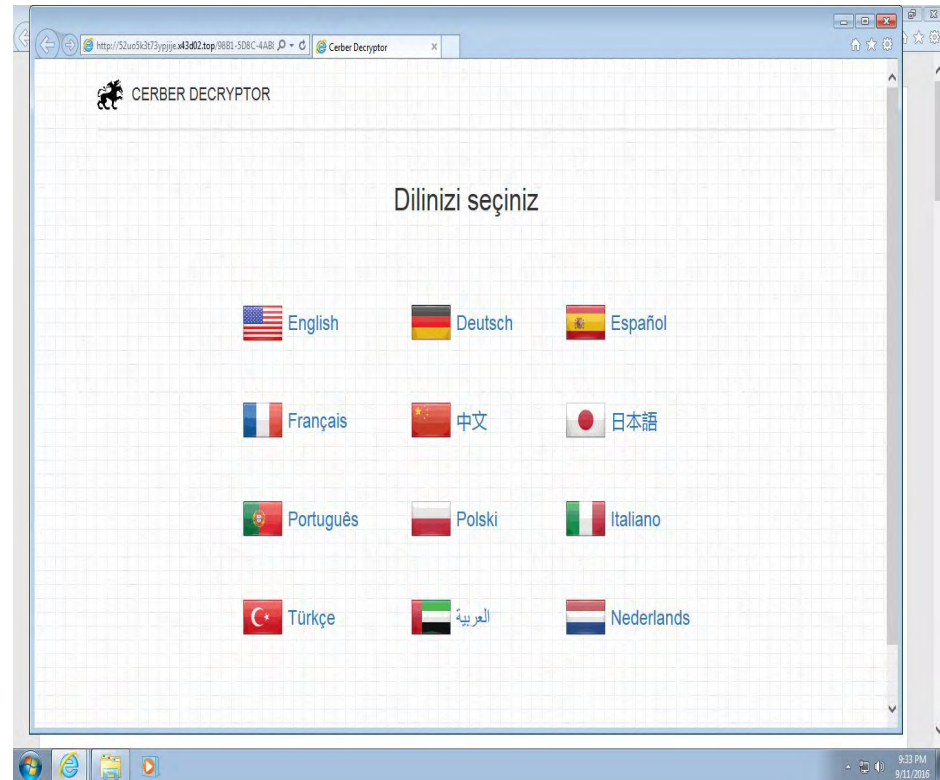
New tricks

- Use of other accepted file extensions (e.g. .WSF, .WSH, .HTA, .PUB files)
 - Bypasses filters that proactively block known dangerous (ZIP) attachments (containing e.g. .EXE, .PDF.EXE, .JS, .DOCM as extension)
- Use of a .DLL file (payload) instead of an .EXE (e.g. Locky/Zepto)
 - In-memory attack; exploit attack delivers no files on the disk
 - Bypasses sandbox, signature and 'math-based, next-gen' products
- Use of other active content in weaponized documents (no macros)
 - e.g. RAA Ransomware
- Use of only trusted binaries, part of the OS (no new code on machine)
 - Bypasses application whitelisting, signature & 'math-based, next-gen' products
- Manipulate timestamp, create extension-less copy, encrypt copy and delete original
 - Cripple / shake off behavior-based monitoring
- Multi-language support by attackers, to help victims pay the ransom
 - Including chat support



Cerber crypto-ransomware

- Ransomware-as-a-service
- Localized e-mail and chat support
- Audio warning

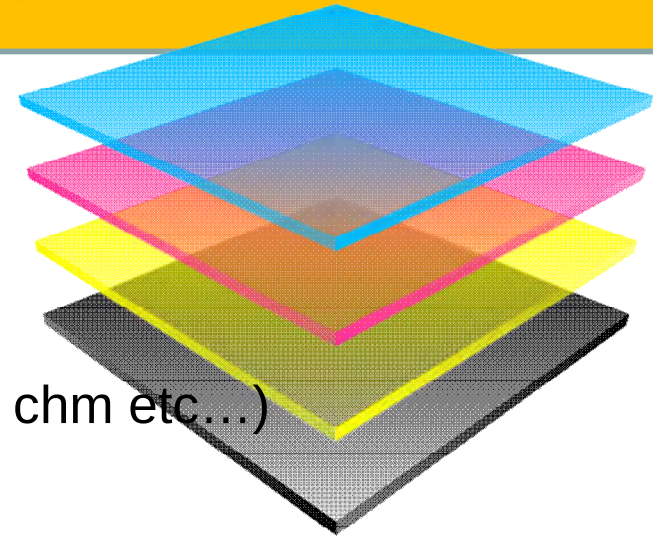


Synchronized Security

Enhancing layered security

As a minimum you should:

- Deploy antivirus protection
- Block spam
- Use a sandboxing solution
- Block risky file extensions (javascript, vbscript, chm etc...)
- Password protect archive files
- Use URL filtering (block access to C&C servers)
- Use HTTPS filtering
- Use HIPS (host intrusion prevention service) & other signature-less technologies
- Activate your client firewalls
- Use a whitelisting solution



Reducing the threat - Additional Steps

Education

Encrypt
Company Data

Use Security
Analysis Tools



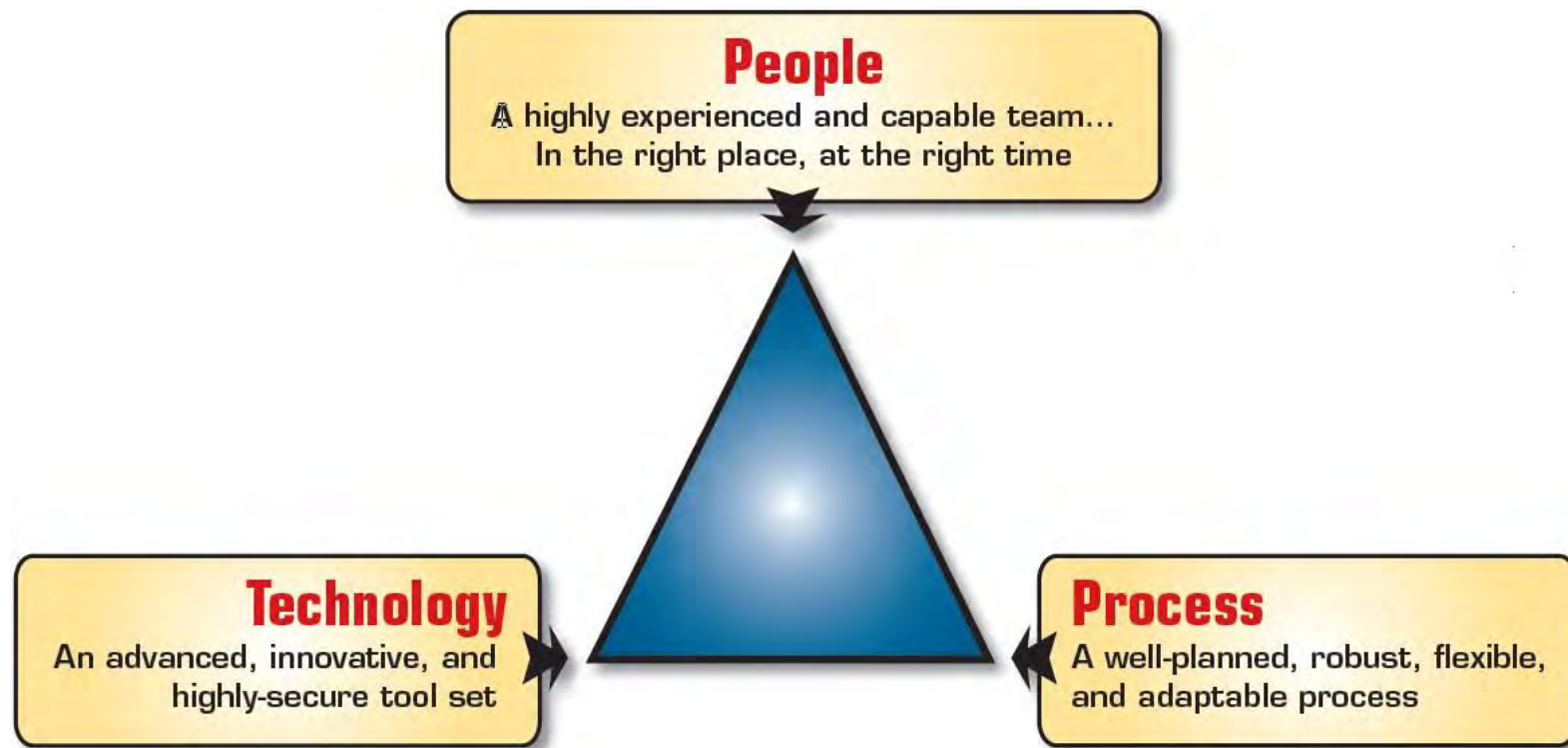
To minimise risks

Management should encourage to comply with International standards:

- 1. Rethink approach to IT security**
 - Proactive approach to threats (rather than responsive)
 - IT security = business enabler, not infrastructure cost
 - Align IT security strategy to corporate risk management objectives
- 2. Update security policies**
 - Organisations need to handle new trends like BYOD, big data, IoT and cloud
- 3. Adopt intelligent multi-layer defence**
 - Application security is important in a Web-centric world
- 4. Maintain up-to-date systems (e.g. patches and regular security audits)**
- 5. Educate user and implement security best practices**



Bottom Line.....PPT



P = People
P = Process
T = Technology



**The weakest
link is..**

PEOPLE

**the
Human Factor**





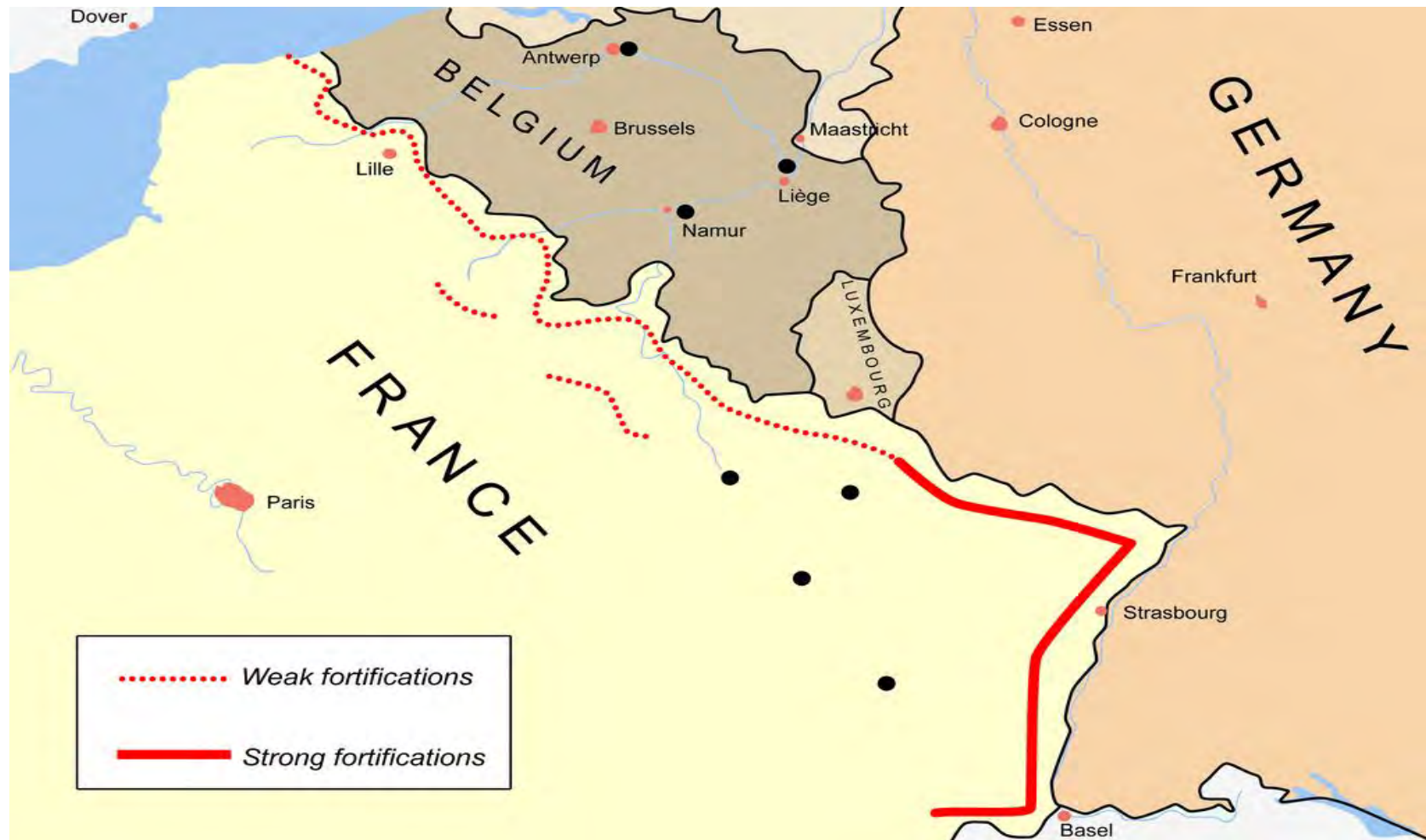
**KEEP
CALM
IT'S
ALMOST
FINISHED**



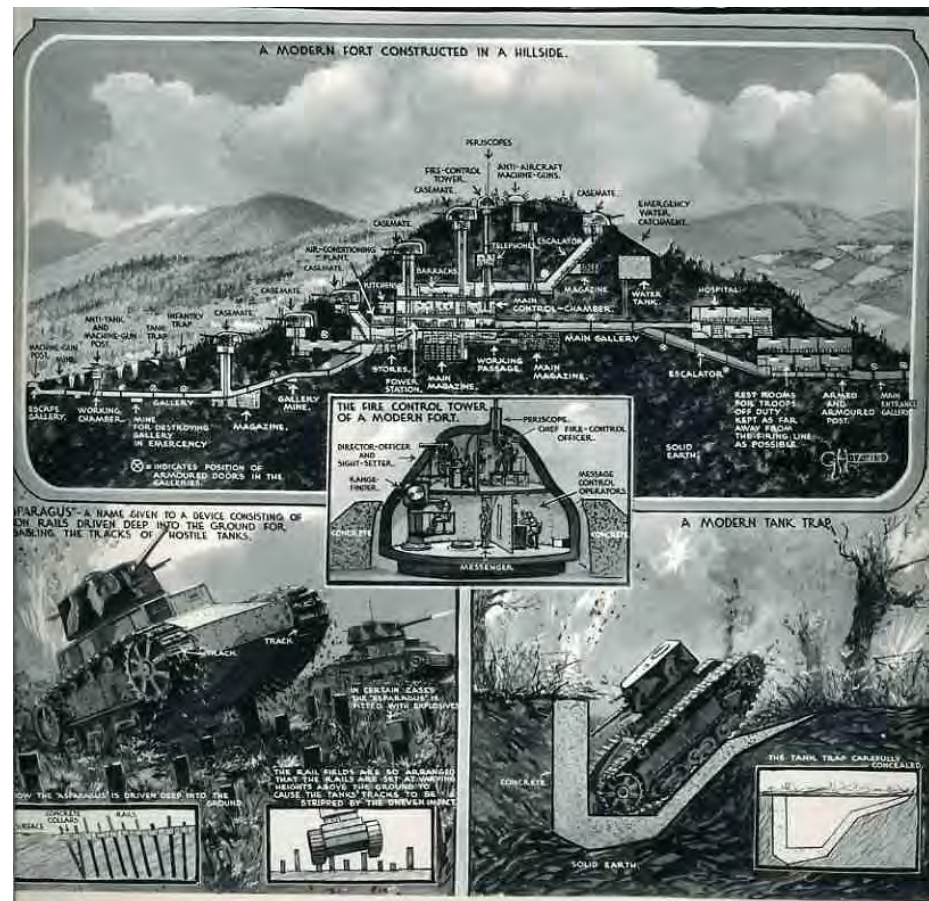
**CYBER RESILIENCE
BUILDING A HIGH
RELIABILITY
ORGANISATION**



Are we building a Maginot line.....



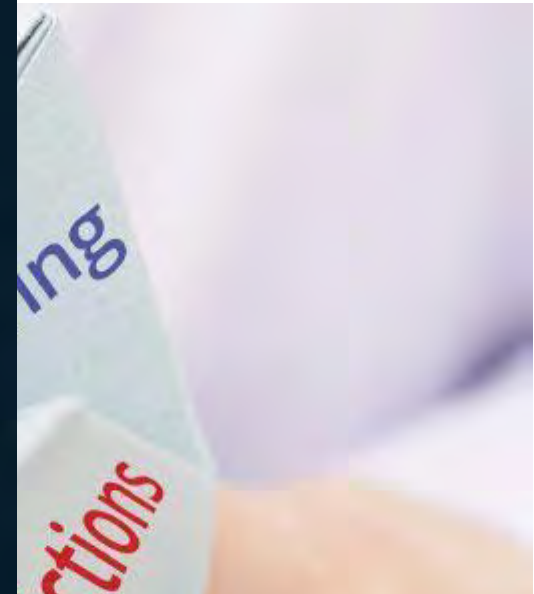
Are we building a Maginot line.....



- 1 : a line of defensive fortifications built before World War II to protect the eastern border of France but easily outflanked by German invaders
- 2 : a defensive barrier or strategy that inspires a false sense of security







Smart contract Blockchain technology



What's in this for us.....

More 2 billion people are connected to the Internet.

Cellular phone subscriptions passing the 5 billion mark at the end of 2010.

More than 50 billion objects are expected to be digitally connected by 2020, including cars, appliances and cameras.

The amount of digital information created and replicated in the world will grow to a staggering amount of 35 trillion gigabytes by 2020.

About USD 8 trillion traded thru e-commerce last year



Takeaways

- ✓ Businesses need to minimize exposure; create systems to protect data; respond appropriately and use insurance to cover response costs.
- ✓ Human beings are inventive; despite the best policies, non-compliance and resulting breaches will occur.
- ✓ Your crisis management skills will serve you well when paired with subject matter experts.

✓ **Issues of cyber risk and data breach that businesses face is not if....but when.**



What's in this for us.....



<https://youtu.be/RBkND76J91k>



<https://www.siliconrepublic.com/companies/2015/11/25/digital-disruption-changed-8-industries-forever>

PART 4

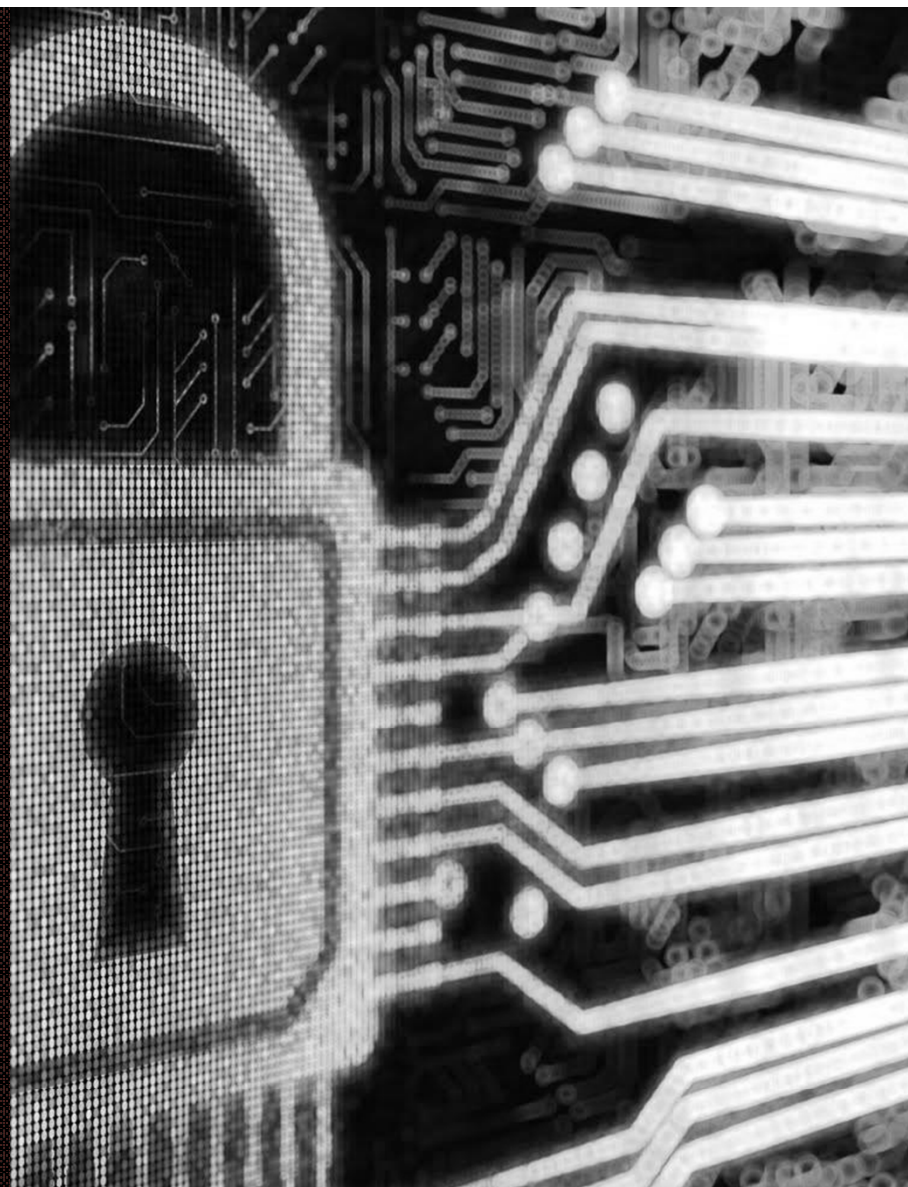


PART 4

UNDERSTANDING CYBER INSURANCE

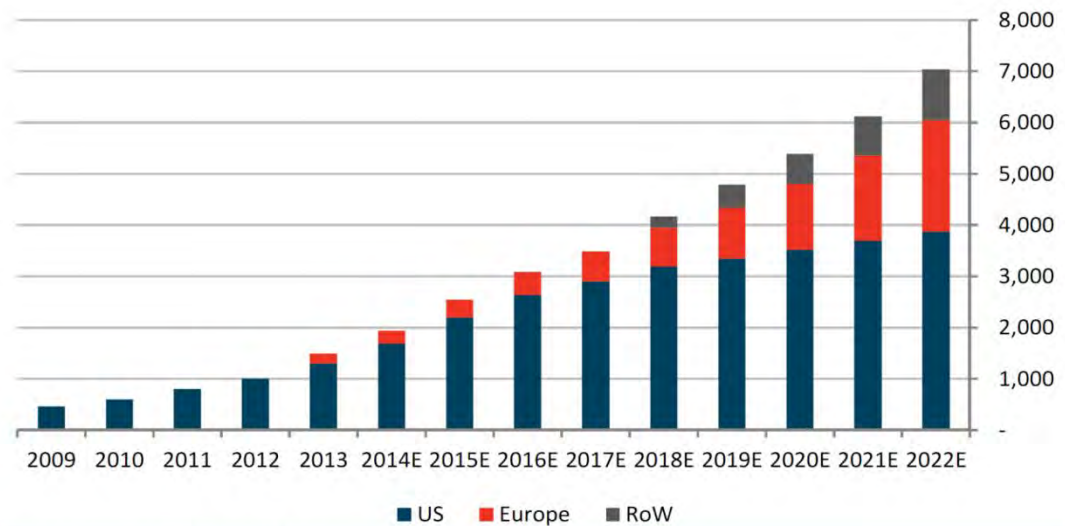
A data breach isn't always a disaster.

Mishandling it, IS!



Why are people so excited about Cyber?

- 2015 global gross premium estimate \$2.5Bn
- 2020 global gross premium projections \$5.5Bn
- 65 Lloyd's Syndicates writing £500m GWP in 2016
- Lloyd's premium approximately 40% of estimated global market
- Lloyd's capacity \$400m
- Global capacity
- Competition



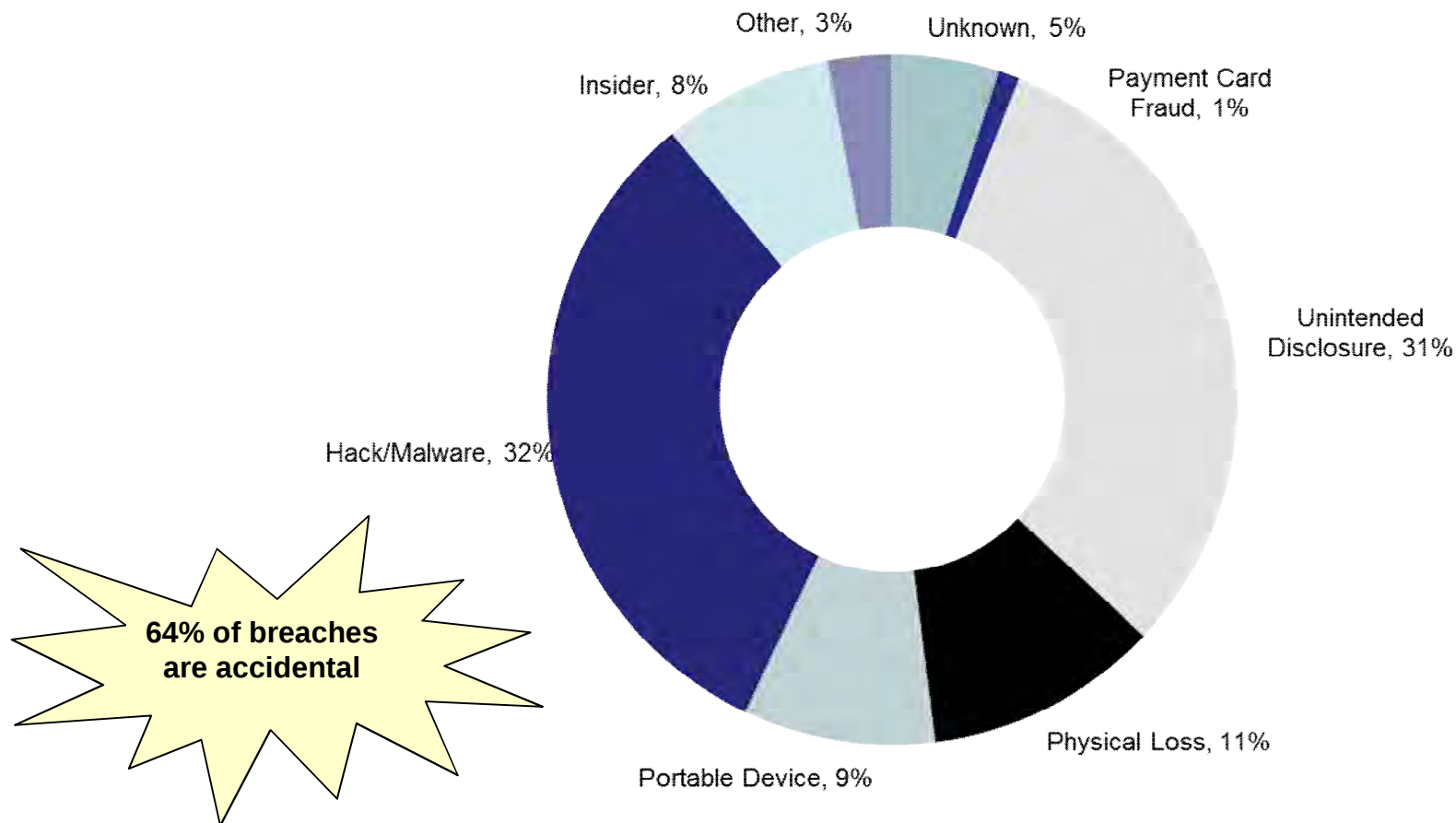
Source: Betterley, Aon, Westhouse estimates



Multiple exposures and causes of loss...



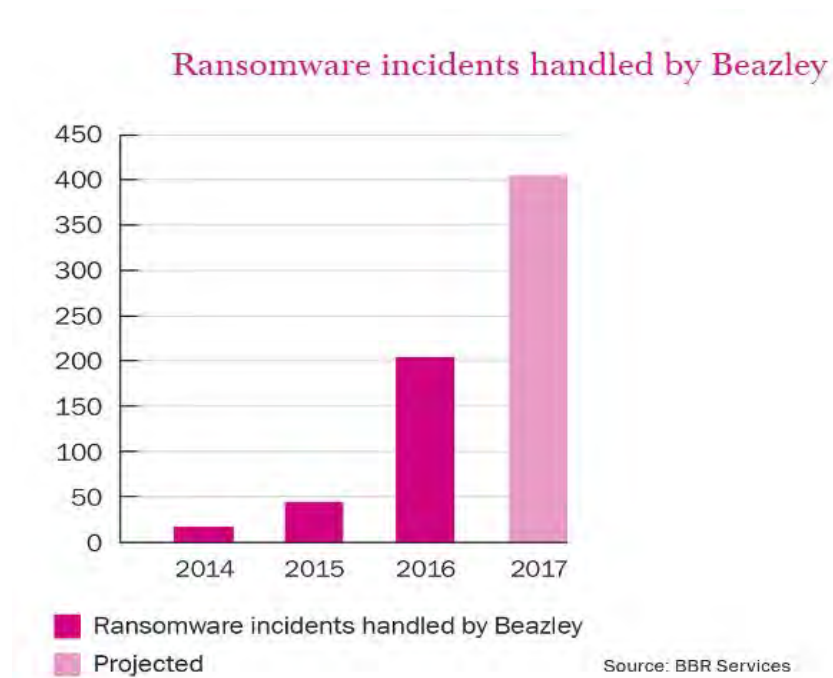
Causes of Loss – by number of breaches



Source: 2016 Beazley Breach Data

Ransomware

Ransomware attacks handled by Beazley more than quadrupled in 2016



Beazley projects these attacks will double again in 2017

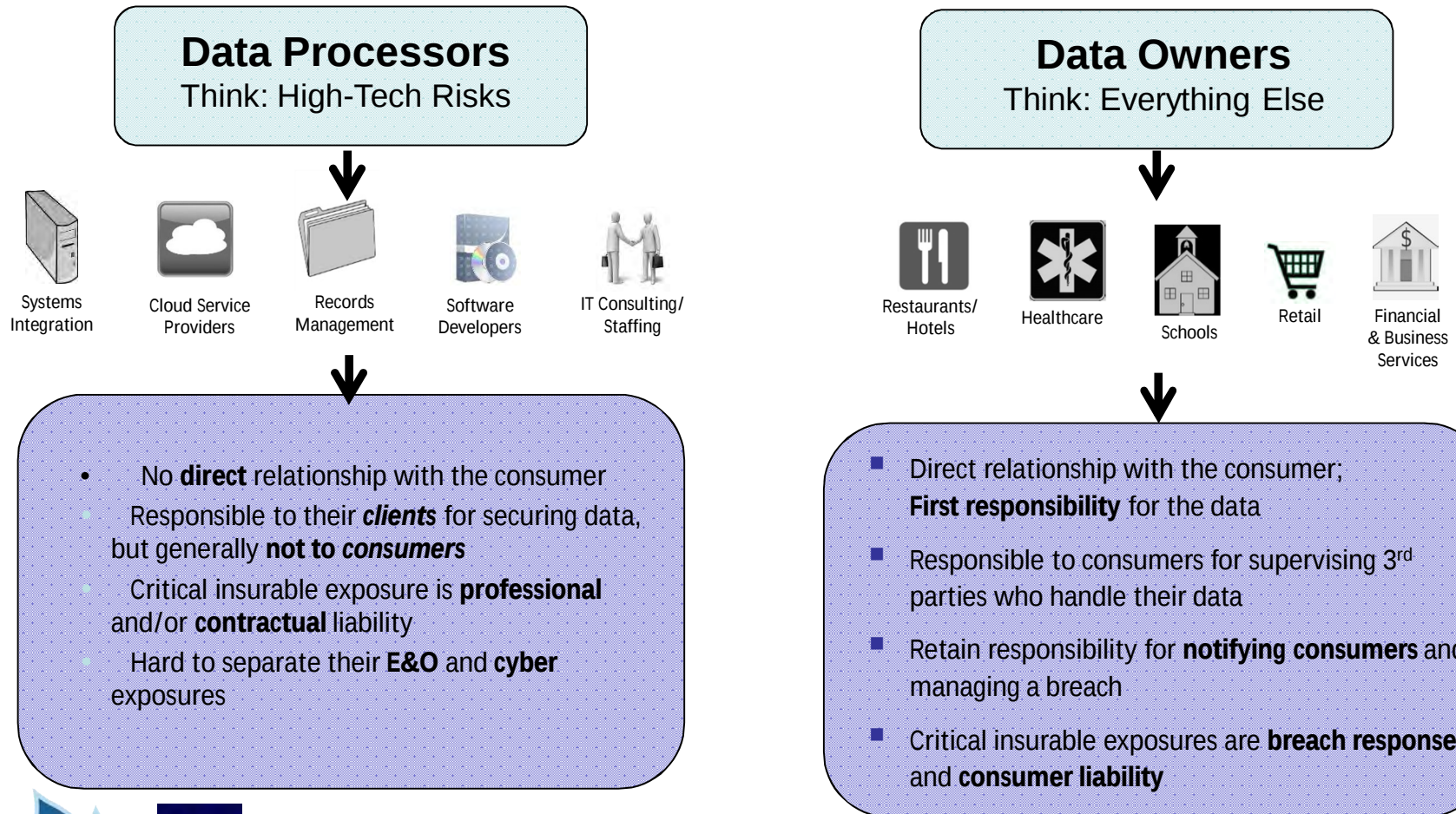




"That's a great question. Come to think of it, I'm not sure what it is I'm trying to sell you."



Data Processors vs. Data Owners – Different Cyber Risks



Impact to business: potential losses – post Cyber breaches

- **Loss of reputation/Customer trust**
 - Financially difficult to quantify
- **Incident clean up**
 - May require expert assistance
- **Third party claims**
 - From clients and individuals
- **Regulatory penalties**
 - Legal requirements
- **Direct revenue**
 - If business is online and website affected



First Party coverages

What Cyber
Insurance covers?

Third Party coverages



First Party Cyber Coverages

- **Data Breach Response Expenses**
 - (a) Forensic investigation costs
 - (b) Legal expenses
 - (c) Notification costs / credit monitoring costs
 - (d) Public relation costs
- **Data Loss and Restoration Costs**
- **Network Business Interruption Loss**



First Party Cyber Coverages

- **Regulatory Defence and Penalties**
- **PCI Fines, Expenses and Costs**
- **Cyber Extortion Loss**

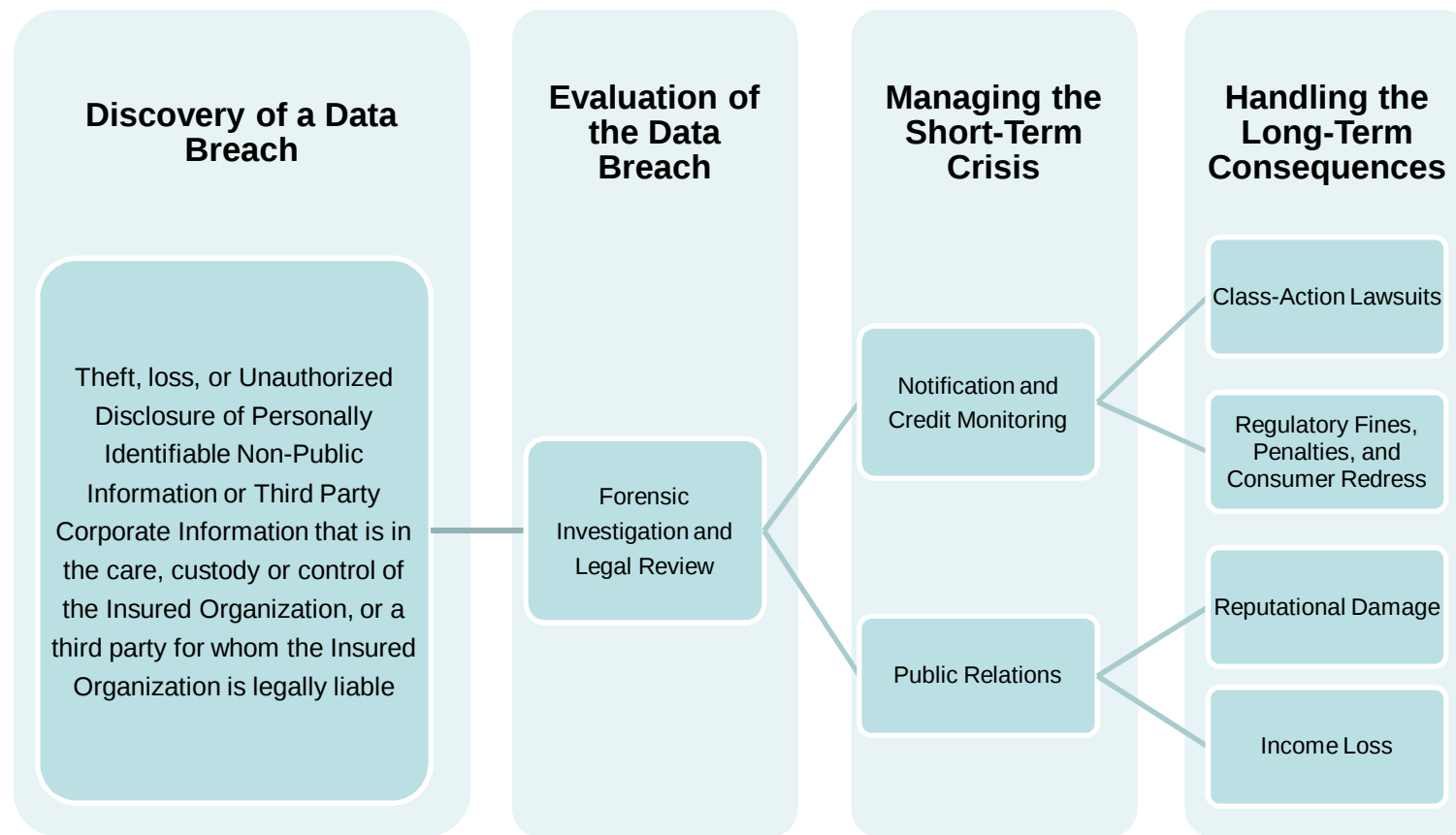


Third Party Cyber Coverages

- **Third-party liability**
 - Information Security and Privacy Liability
 - Legal liability, defense costs and expense reimbursement for liability from unauthorized disclosure of PII or third party corporate information
 - Network Security Liability
 - Failure of computer security to prevent a security breach
 - Website Media
 - Liability for online media activities
 - o Defamation, copyright infringement, infringement of trademark
 - o May include offline media
 - Judgments / settlements
 - Defense costs – litigation



Chronology of a Data Breach



Computer Forensics & Privacy Counsel STEP 1

- **Computer forensics** investigation to determine scope and depth of breach
 - The total computer forensic price can average from **\$250 to \$350 an hour**, and the process involves three basic steps:
 1. Acquisition or harvesting of all electronic information: **30 Hours**
 2. Investigation and examination of all information: **15-35 Hours**
 3. Reporting: **15 hours**
- **Privacy counsel**: to advise how to respond to various privacy notification statutes
 - Important to use experienced privacy counsel to navigate the breach laws of 47 states and the various federal statutes
 - Billing rates range by city but average **\$350-\$1,000 per hour**.



Why forensics is important

- Entity Affected: Financial Services Firm
- Incident Details: Company suffered a malware intrusion and initially believed all 280,000 customers' PII was compromised. Forensics reversed engineered the malware to determine it was only collecting credit card numbers beginning with "3". (American Express Cards) Without Forensics, the company would have notified the entire population.
- Data Format: Electronic
- Information Compromised: Name, Credit Card #
- Breach Universe: 30,000+



Post Breach Response

STEP 2

- **Notification vendor / Call center** if necessary and required to be complied
- **Credit monitoring:** Remedy offered to affected individuals
 - **\$30/person** for 1 year of monitoring
 - Credit restoration services offered to victims of fraud
- **Public Relations** specialist: to handle the reputational fallout



Don't assume you know the facts

- Entity Affected: Hospital
- Incident Details: Hospital did a “disaster drill”. Set up 20 laptops, one in each ER suite. To replicate lost power, each laptop was to be set up with all 500,000 EHRs of the hospital. During course of drill, 1 laptop went missing.
- Initial Response: Hospital called a press conference to acknowledge a loss of 500,000 EHRs. They held the press conference BEFORE the investigation.
- Investigation: Investigation identified time of loss via surveillance cameras in the ER. IT reviewed network logs for downloading the 500,000 EHRs to each laptop and noticed 1 laptop did not receive the 500,000 EHRs. Investigation took 48 hours.
- Conclusion: It was forensically concluded that the missing laptop was stolen BEFORE the download of 500,000 records occurred.
- Data Format: Electronic
- Information Compromised: PHI
- Breach Universe: ZERO – “Non-Event”
- Aftermath: The hospital had to hold a second press conference about the “false alarm”.



Typical Breach Response Costs

- **Response costs** – sending out notices, call center services, and the offer of credit monitoring:
 - \$30 - \$50 per record
- **Forensics**, to determine the size and scope of the breach:
 - \$25,000 to more than \$500,000
- **Privacy Counsel:**
 - \$25,000 to more than \$100,000

• *A small clinic that sees 200 patients a week and retains records for 10 years would have to notify over 100,000 patients, costing upwards of \$3,000,000 for notification and credit monitoring alone.*



Most Breaches are
NOT caused by
hacking

Even the best IT
security can't keep up

Employees drive 75%
of all data breaches



Wrap-up



“It’s not a matter of if... it’s a matter of when”



What's a company to do?

1. **Get a checkup** – Evaluate current protections, identify weaknesses through a cyber risk assessment.
2. **Educate your employees and senior leadership** – People are your weakest security link. Stolen (or weak) credentials, social engineering, removable media, portable devices are keys to cyber threat.
3. **Prepare to respond** – Establish a response plan before you have an attack. Involve key stakeholders; consider all sources of data breach. Buy Insurance.
4. **Repeat steps 1-3** – Cybersecurity landscape is changing rapidly. Attacks are evolving, response plan needs to evolve accordingly



PART 5

- Specimen policy wording
- Proposal form (underwriting requirements)



ACKNOWLEDGEMENTS

- 1) Wayne Griffith (P&O Insurance)
- 2) Cyber Security Malaysia
- 3) Shan Sagoo (ARB)
- 4) Beazley Limited and other Lloyds Syndicates
- 5) Kevin Rajah

THANK YOU!

