Cyber-Security Nightmares - Security Incident Response & Investigation

Tales from the Trenches


R
RESTRICTED
UNDER 17 REQUIRES ACCOMPANYING
PARENT OR ADULT GUARDIAN
VIOLENCE, GRISLY IMAGES, LANGUAGE,
SOME NUDITY AND SEXUALITY

AGENDA

- Introductions
- Sources & Types of Security Breaches
- Case Studies
- Recent breaches
- Preparing for the Inevitable Privacy and Security Incident
- What to do in the event of a breach
- Lessons learned
- Q&A

Consulting Practice Overview

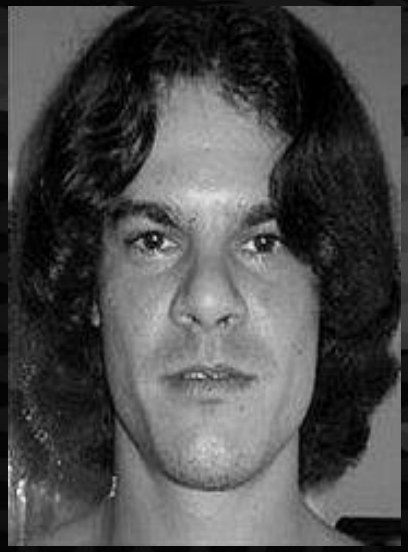
- Focused Technology Security Group since 2002
- Experienced team of I.T Security Talent
- All aspects of Security
  - I.T. Security best practices
  - Technical security audits
  - Physical security
  - Covert operations
  - Cyber Security Investigations & Forensics

You Will be Hacked!

Why?

You don’t get shot robbing banks on-line!

Sources Of A Breach



Organized Criminal

Well Meaning Insider

Malicious Insider

Common Types of Data Security Breaches

Cybercrime Hacking: in this type of breach an external hacker accesses your organizations network and ***obtains unauthorized access to sensitive patient information. Includes ransomware attacks.***

Loss or Theft of Mobile Device or Media: in this type of breach a worker either loses or has stolen a mobile device or media containing sensitive data, ***resulting in potential unauthorized access to that data and a breach.***

Insider Accidents or Workarounds: in this type of breach a worker performs a well-intentioned action that results in unauthorized access to sensitive information. ***A common example of this type of breach involves a worker emailing unsecured sensitive information, resulting in potential unauthorized access to this information, and a breach.***

Common Types of Data Security Breaches

Business Associates: in this type of breach a third party organization contracted by your organization experiences a breach event involving unauthorized access to sensitive corporate information. ***In this case the information impacted originates from your organization and was previously shared for the purpose of the third party organization fulfilling its contractual obligations.***

Malicious Insiders or Fraud: in this type of breach a worker performs a malicious action that results in unauthorized access to sensitive corporate information. This could be a disgruntled worker, or done for the purpose of committing fraud. ***A common example of this type of breach involves fraud where a worker sells sensitive corporate information on the black market.***

Common Types of Data Security Breaches

Insider Snooping: Insider snooping involves a worker accessing the records of taxpayers or other employees of your organization without any legitimate need to do so***, for example where a disgruntled employee might suspect they are going to be disciplined.***

Improper Disposal: in this type of breach an electronic device or media containing sensitive corporate records is not properly decommissioned. In particular, the sensitive information is not securely wiped or destroyed before disposal. ***Example of this are discarding or selling electronic devices that have corporate information stored on them, or discarding paper based records without first shredding them.***

Common Types of Data Security Breaches

Social Engineering: *Social engineering, in the context of security, is understood to mean the art of manipulating people into performing actions or divulging confidential information.*

- Phishing via email
- Phone phishing
- Diversion methodologies including physical security

Common Types of Data Security Breaches

Phishing via email – Case Study 1

- Very successful – almost 100% success rate if crafted professionally. Results in Malware attacks, including Ransomware.

- Recent attack resulted in major permanent loss of data – Backups were corrupt!

  - In summer of 2016, accounting department contacted help desk after detecting some files are not readable.
  - Subsequently over 2000 files were found to be corrupted, across three servers.
  - Based IT staff's research, it was determined to be Ransomware, and these corrupted files were actually files that got encrypted by Ransomware.
  - Wordsworth & Associates attended and user PC's were found to be infected with CryptoWall Ransomware.
  - All PCs and servers had Norton Endpoint protection installed, which according to Symantec should detect CryptoWall.
  - The fact that it didn't detect anything indicated a deeper compromise which may have somewhat disabled Norton.

Common Types of Data Security Breaches

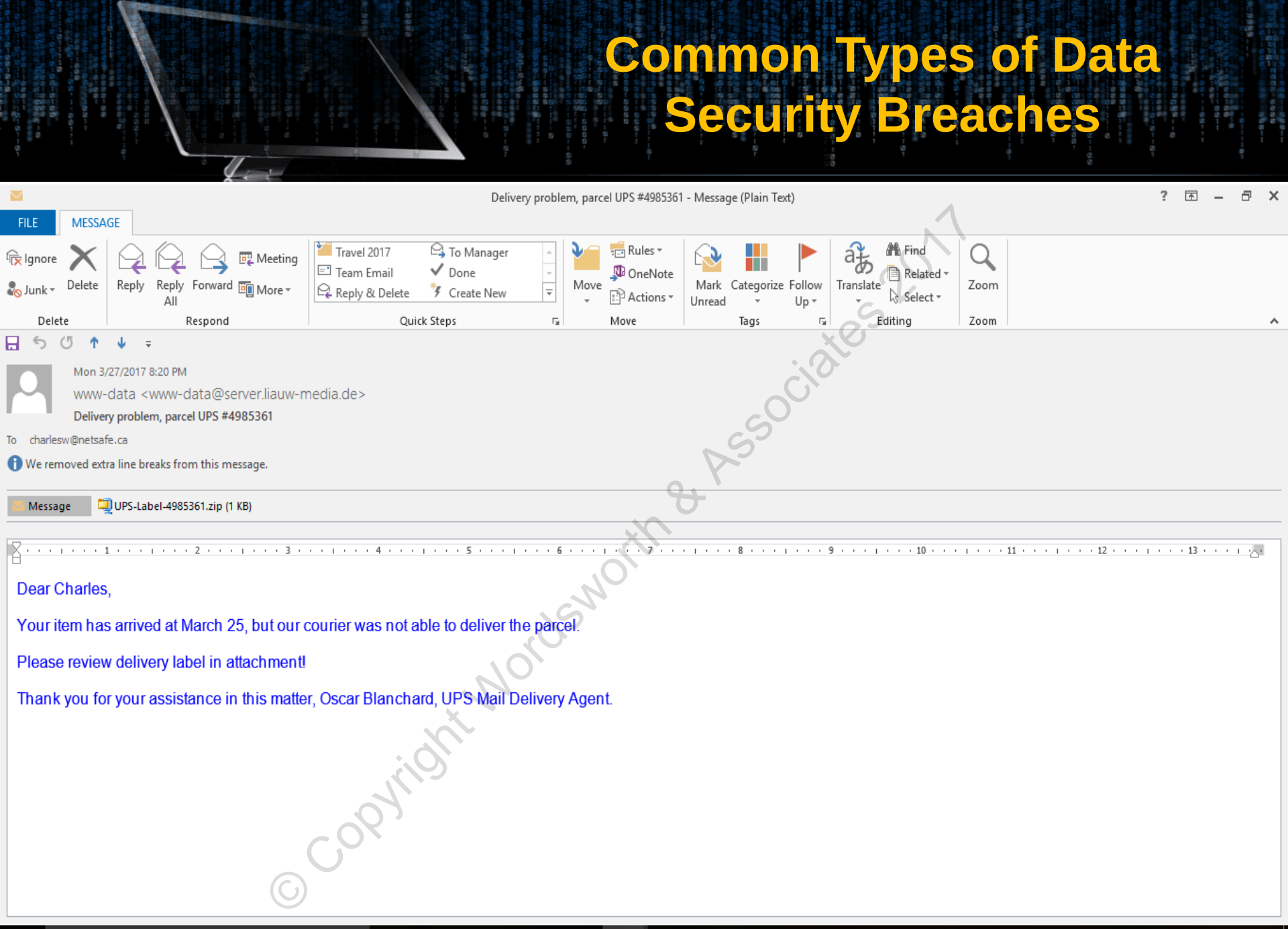
Phishing via email – Case Study

- Prior to W&A arriving on site, the company pulled the plug on the Internet and on the affected servers

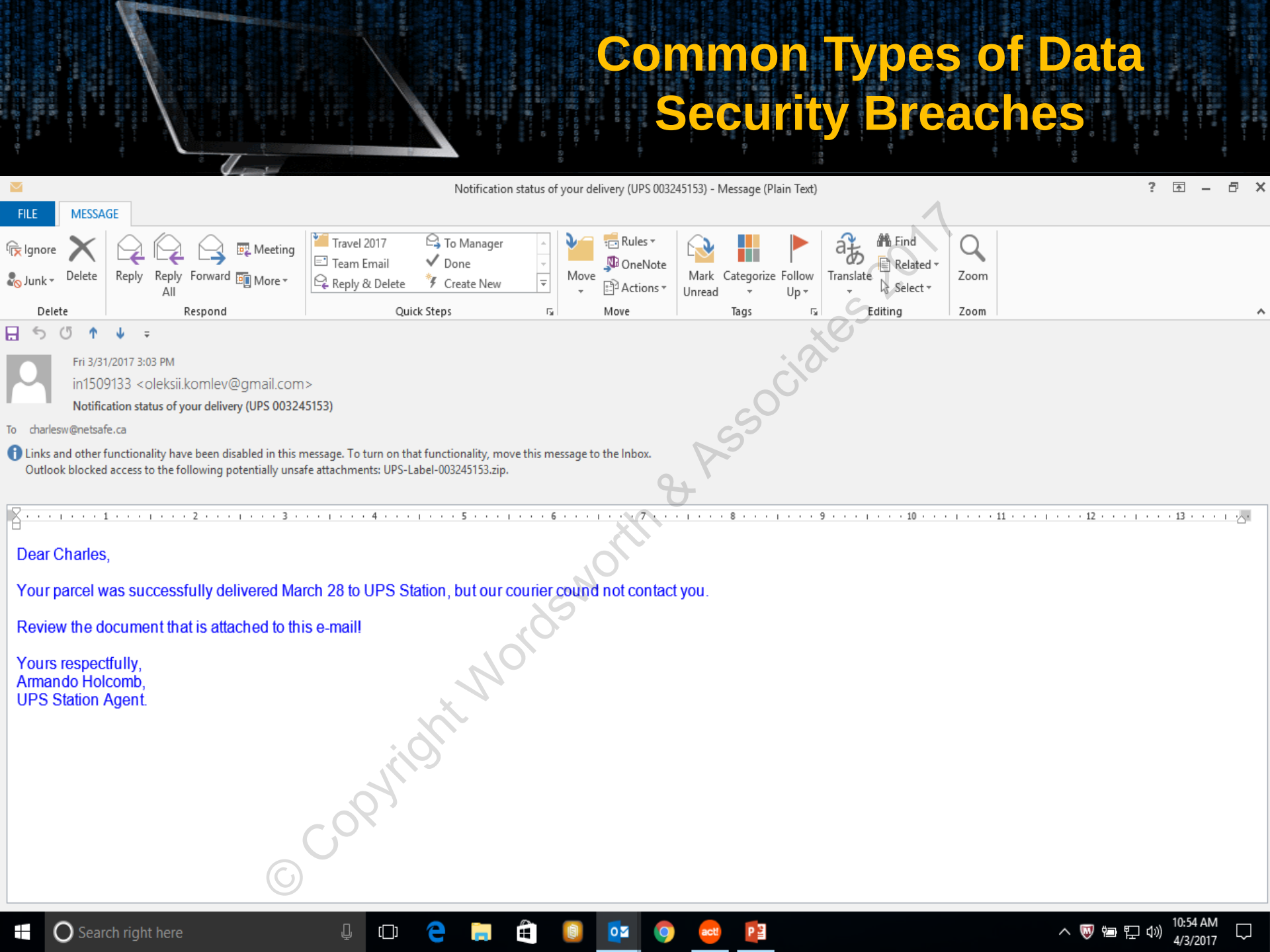
The company was NOT presented with the usual Ransomware screen (see example left:

Common Types of Data Security Breaches

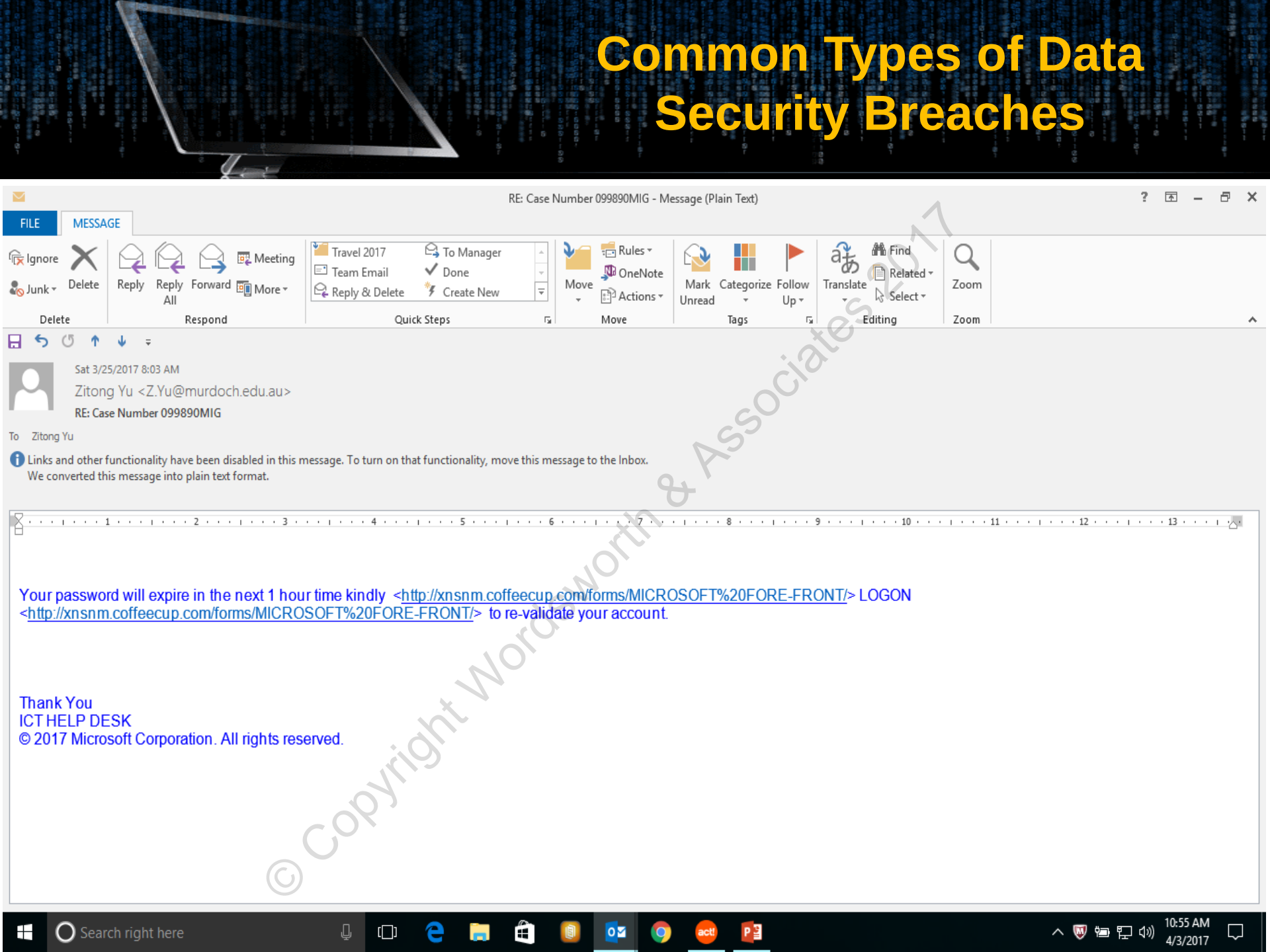
Common Types of Data Security Breaches



Common Types of Data Security Breaches



Common Types of Data Security Breaches



Common Types of Data Security Breaches

Phishing via email – Case Study 1 - Conclusion

- Ransomware was installed as a result of phishing attack – user clicked link
- Backup procedures were inadequate – some backups were corrupt and un-tested
- Had the Company been presented with the Ransomware screen they might have paid the ransom and recovered their files
  - *However the Company might never had discovered they had corrupt backups*
- Company had never had an independent IT security audit
- Employees had not received security awareness training
- Company had no Disaster Recovery, Incident response or Business Continuity Plan

Heads up !

- *Set up a Bitcoin account*
- *Negotiate with the hacker*

Common Types of Municipal Data Security Breaches - Internal

Result:
You are PWND!!

Common Types of Municipal Data Security Breaches

External attack via Wifi - Case Study 2

W&A Auditors sat in vehicle in parking lot

Common Types of Municipal Data Security Breaches

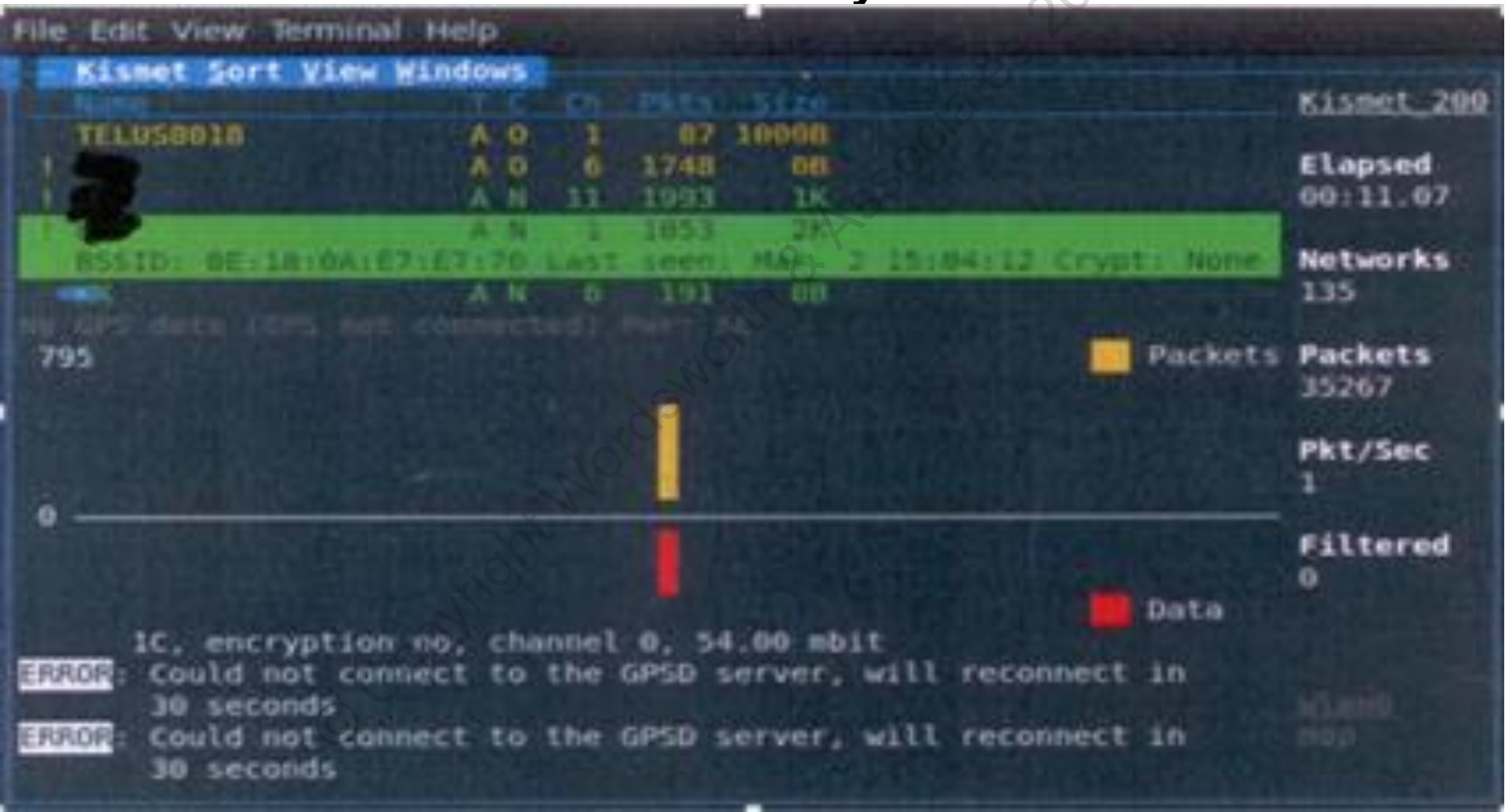
External attack via Wifi - Case Study 2

W&A Auditors sat in vehicle in parking lot

- **Completed covert Wifi survey**
- **Observed various corporate Wifi networks**
- **Observed a staff member accessing Wifi network**

Common Types of Municipal Data Security Breaches

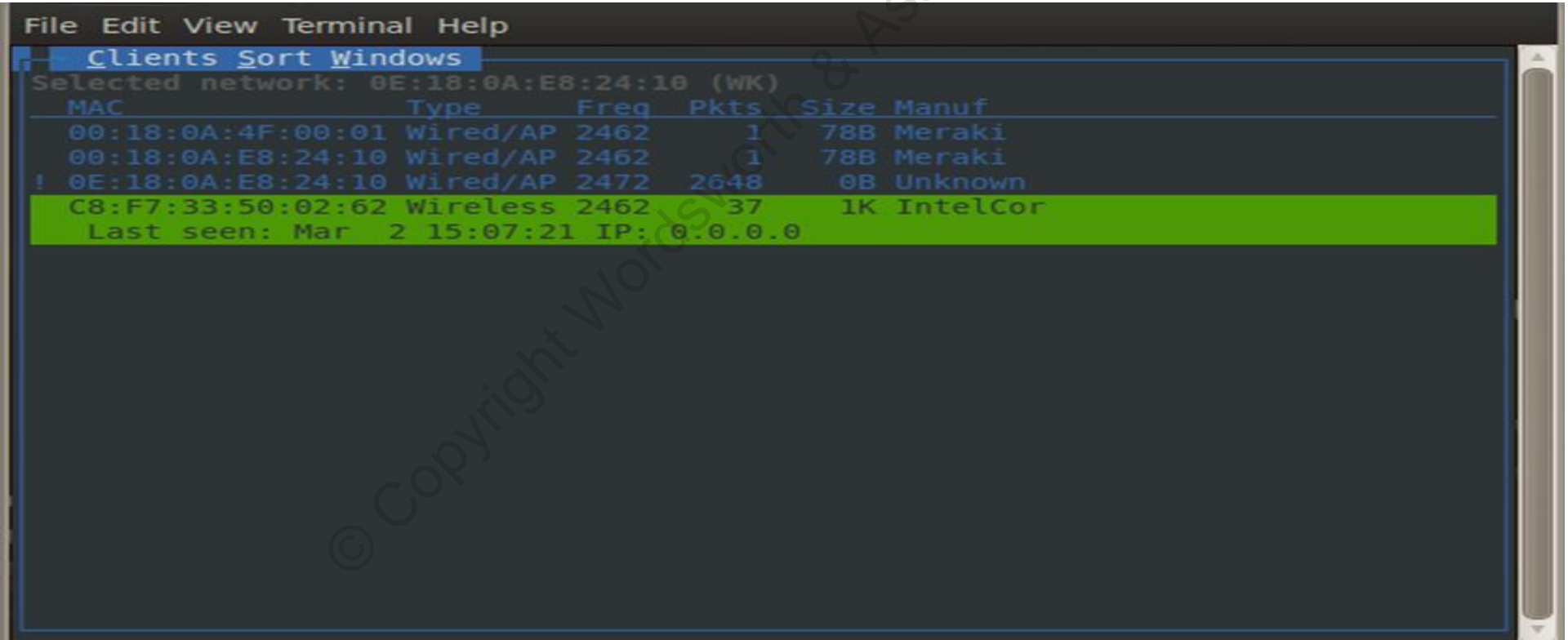
External attack via Wifi - Case Study 2



Common Types of Municipal Data Security Breaches

External attack via Wifi - Case Study 2

Utilizing macchanger, the auditor could easily manipulate the MAC address on user laptop!



Common Types of Municipal Data Security Breaches

External attack via Wifi - Case Study 2

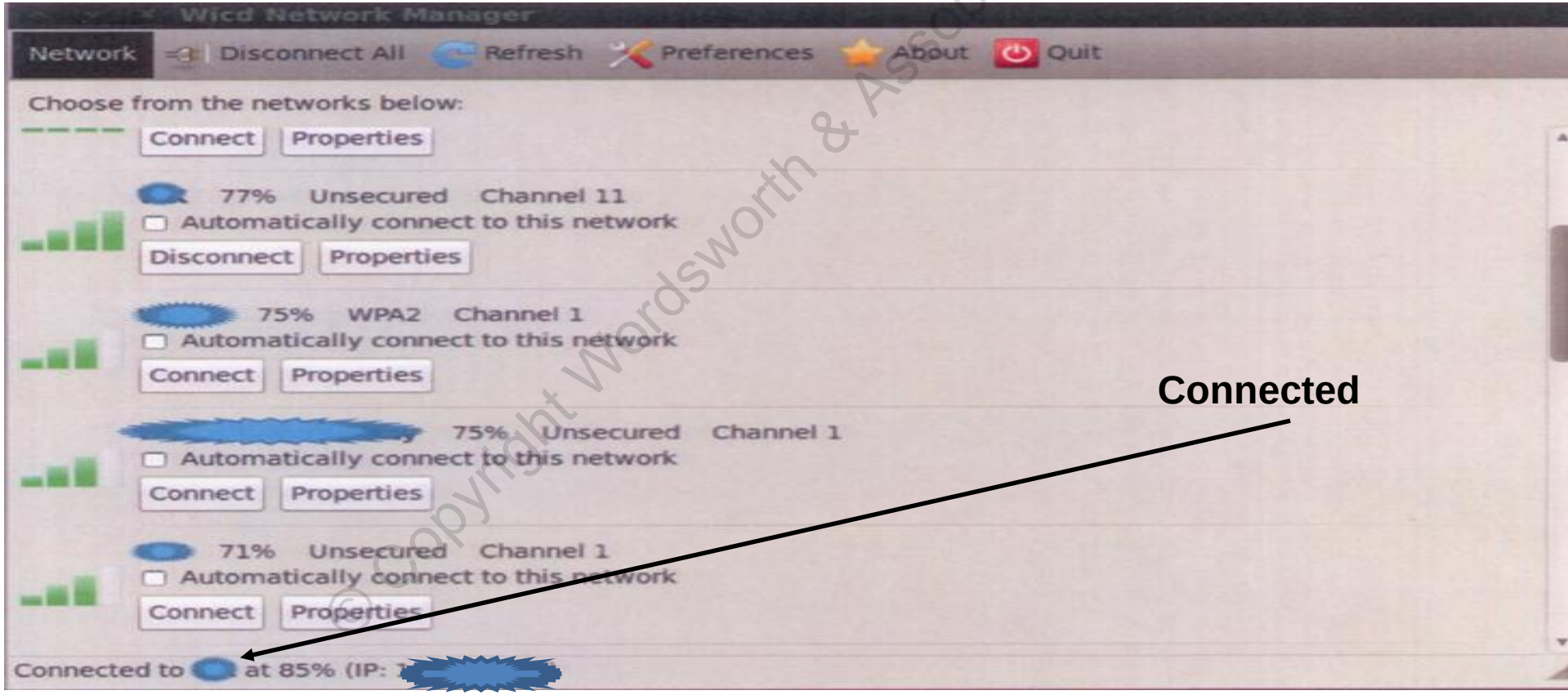
********** Change MAC address on auditor's laptop **********

```
# ifconfig wlan0
wlan0     Link encap:Ethernet  HWaddr 00:26:5e:fe:47:ae
          UP BROADCAST PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

# macchanger --mac=c8:f7:33:50:02:62 wlan0
Current MAC: 00:26:5e:fe:47:ae (unknown)
Faked MAC:   c8:f7:33:50:02:62 (unknown)

# ifconfig wlan0 up
root@bt:/home/201702-cwk/wifi# ifconfig wlan0
wlan0     Link encap:Ethernet  HWaddr c8:f7:33:50:02:62
          UP BROADCAST PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Common Types of Municipal Data Security Breaches

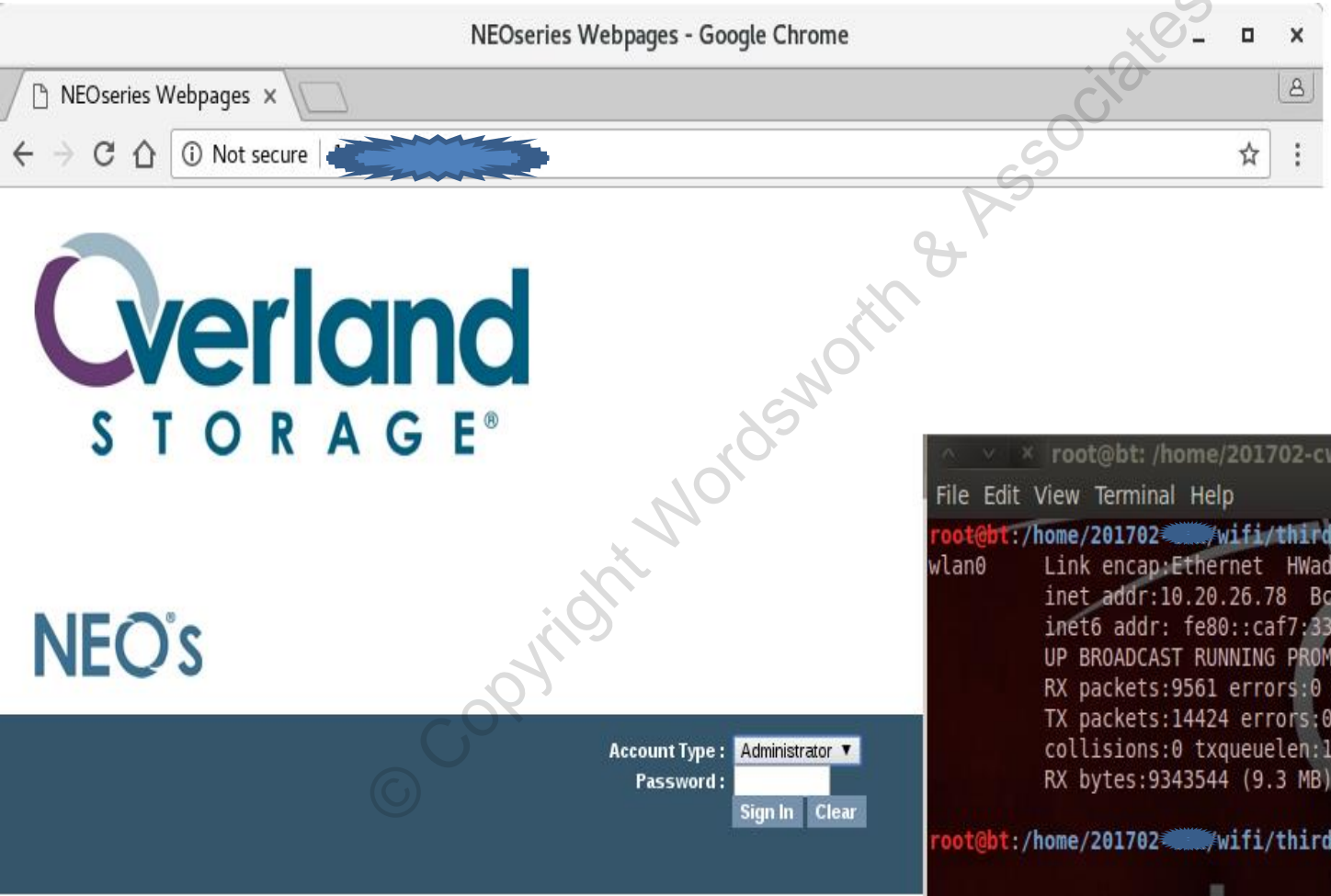
External attack via Wifi - Case Study 2

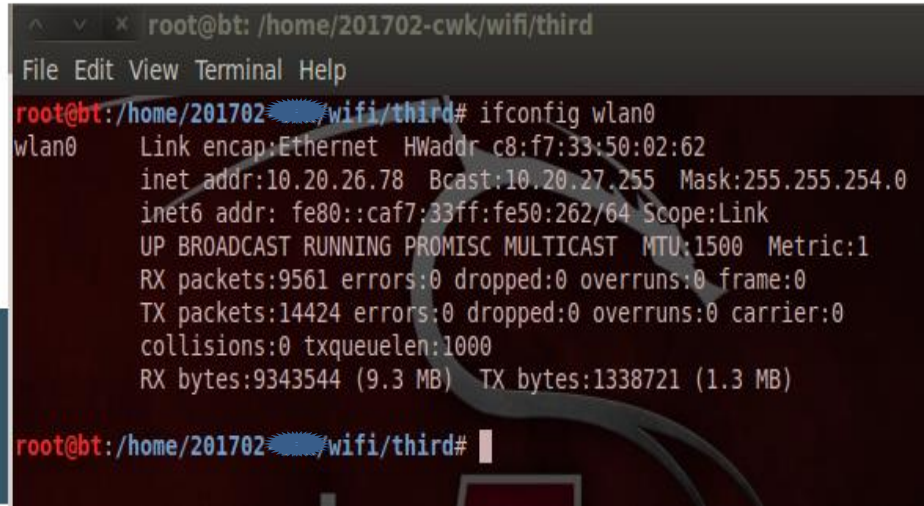
The auditor was then able to log on to the City Wifi internal network



Common Types of Municipal Data Security Breaches

External attack via Wifi - Case Study 2





Common Types of Municipal Data Security Breaches - Internal

Result:
You are PWND!!

Common Types of Data Security Breaches

Internal attack utilizing MITM attack - Case Study 3

- **Wordsworth & Associates Technical Auditors were engaged to covertly examine internal network of corporation**
- **Arrived on site and set up in board room**
- **Covertly connected to corporate network**
- **Used “sniffer” (surveillance) software to examine network traffic**
- **Launched “Man in Middle Attack”**

Common Types of Data Security Breaches

Internal attack utilizing MITM attack - Case Study 3

- The **Man-In-the-Middle (MITM) attack** is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is being intercepted by the attacker.
- During a MITM attack, a malicious attacker will use this technique to force specific network traffic to be re-routed transparently past his or her workstation.
- The goal is to capture any useful data that might not normally be accessible, including login IDs and passwords that can be reused later.

Common Types of Data Security Breaches

Internal attack utilizing MITM attack - Case Study 3 - Capturing password hashes.

**************** MITM towards [redacted] subnet using LLMNR poisoning ****************

[redacted]K:e3204a7907c81a84:35CC9C70F01BD07069EEECF72E8E5126:0101000000000000058C067143C94D2017D0EEB1
344C1C7FC0000000002000E004E004F004D00410054004300480001000A0053004D00420031003200040000A0053004D0042003
100320003000A0053004D00420031003200050000A0053004D004200310032000800300030000000000000000000000002000003
3B6449ABB14B2AF80D9A1735A23AA1D71A1CBBE206D56E0B0936975E72223340A001000000000000000000000000000000000
000090014006300690066007300 2F0075007400690006C003200000000000000000000 ← NTLMv2 hash

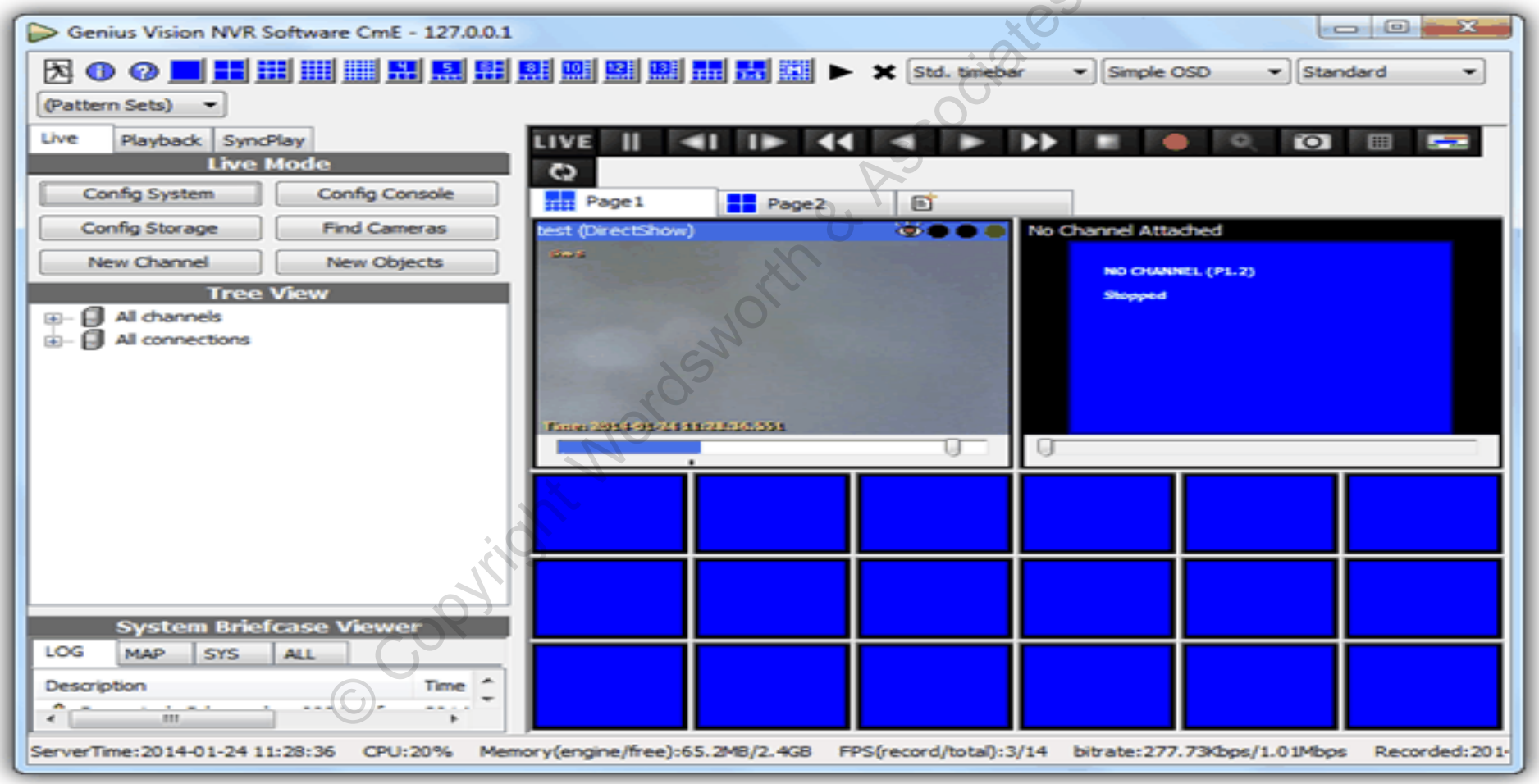
[redacted]WK:4f588dc95ff8735d:FEA397BFC59D01C075EB64E309F771E7:0101000000000000C0653150DE09D201C090D8E
07C4CEAF700000000020008005300 4D004200330001001E00570049004E002D005000520048003400390032005200510041 0046
005600040014005300 4D00420033002E006C006F00630061006C000300340057004900 4E002D0050005200480034003900320 05
2005100410046005 6002E0053004D00420033002E006C006F00630061006C000500140053004D00420033002E006C006F00630
061006C0007000800C0653150DE09D2010600040002000000080030003000000000000000000000000000200000C899FC26C324B
9ED021F73D482A738FDBAA51AB3CE5535B097560E3D8751A6F40A001000000000000000000000000000000000000000009001A006
3006900660073002F0064006F007700730061006E00300032000000000000000000000000000 ← NTLMv2 hash

[redacted]K:2656dc94e6587b02:F7774D36C6B09AABA4E456F49231CC42:0101000000000000C0653150DE09D201E
2F8E9B54F9BEFE3000000000200080053004D004200330001001E00570049004E002D005000520048003400390032005200510
04100460056000400140053004D00420033002E006C006F00630061006C000300340057004900 4E002D0050005200480034 0039
003200520051004100460056002E0053004D00420033002E006C006F00630061006C000500140053004D00420033002E006C00
6F00630061006C0007000800C0653150DE09D20106000400020000000800300030000000000000000000000000002000003CC58D
8A5B50B06256D55CE0F9BB900A1F6F22CFF0BEDF0F0ABFEE56FB62695E0A0010000000000000000000000000000000000000000
9001400630069006600 73002F0075007400690006C003200000000000000000000000000 ← NTLMv2 hash

Common Types of Municipal Data Security Breaches

Internal attack utilizing MITM attack - Case Study 3

- Accessing CCTV video console



Common Types of Municipal Data Security Breaches

Internal attack utilizing MITM attack - Case Study 3 - Capturing live video feeds

Common Types of Municipal Data Security Breaches

Internal attack utilizing MITM attack - Case Study 3 - Capturing live video feeds

Common Types of Municipal Data Security Breaches

Internal attack utilizing MITM attack - Case Study 3 - Capturing live video feeds

Common Types of Data Security Breaches

Phishing via email – Case Study 3 - Conclusion

- All network traffic was unencrypted (Clear Text protocol)
- Company network personnel unaware we were on their network
- Users were unaware we were collecting user names & passwords
- Users were unaware we were listening in to their phone calls (via VOIP)
- We logged onto their CCTV security & teleconferencing system
- We logged onto their building management system
- Company had never had an independent IT security audit
- Employees had not received security awareness training
- Company had no Disaster Recovery, Incident response or Business Continuity Plan

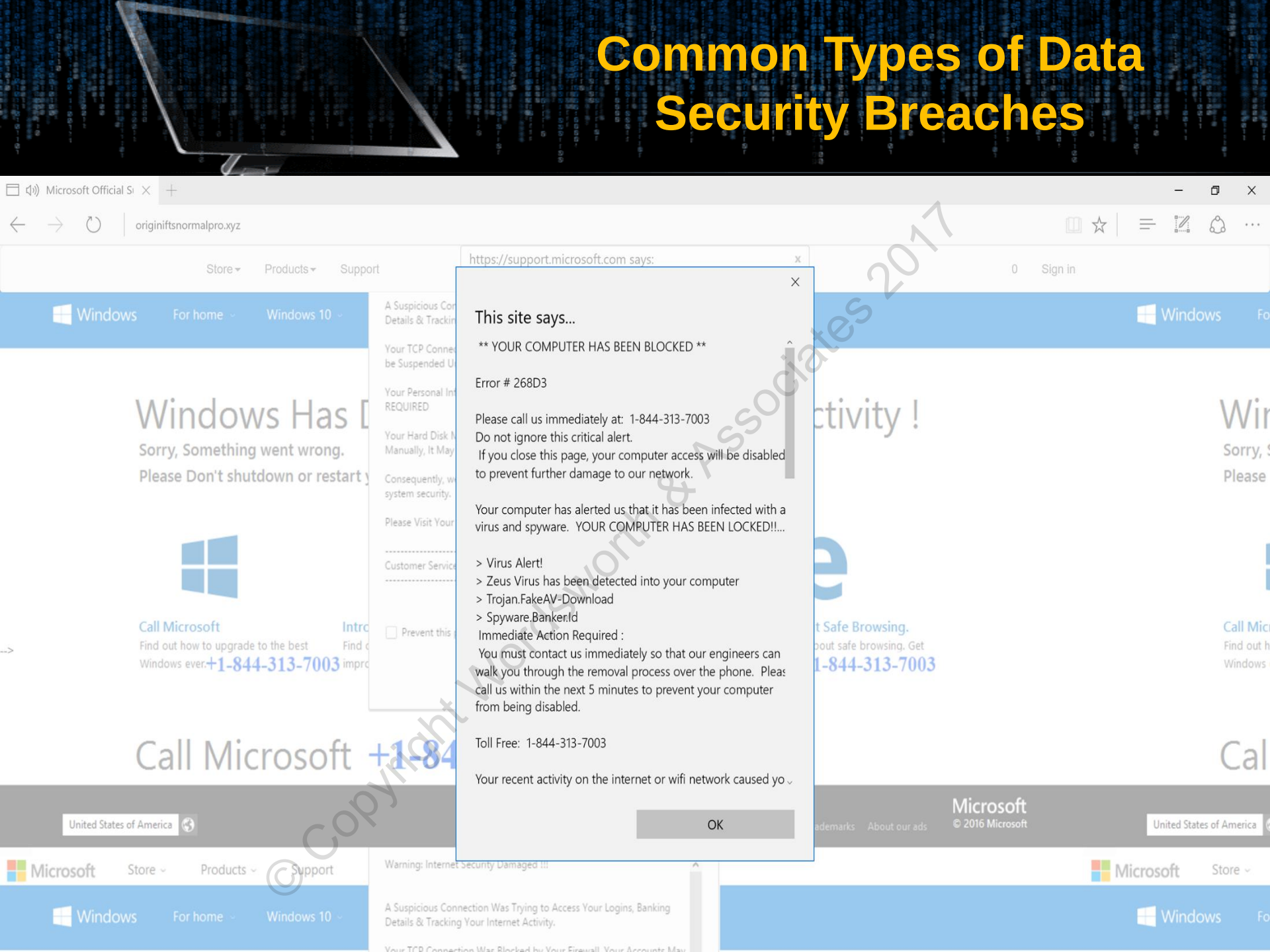
Heads up !

- *Encrypt all network traffic, including VOIP*
- *Complete Independent I.T. security audit*
- *Develop Disaster Recovery, Incident response or Business Continuity Plan*

Common Types of Municipal Data Security Breaches - Internal

Result:
You are PWND!!

Common Types of Data Security Breaches



Common Types of Data Security Breaches

Recommendations:

Primarily hitting home users.

Don’t call the 1 800 number!

- *Power down the PC*
- *Power up PC and run anti-virus program*
- *Clear browsing history, cookies & cached images from browser*
- *Educate family*

Common Types of Data Security Breaches

Social engineering – Case Studies

It is very easy to use physical security activities to access corporate facilities:

- **Very often there are holes in the physical security of the enterprise**
  - No alarm system
  - No CCTV cameras
  - Trusting employees
  - Employees not trained in physical security
  - Tailgating employees
  - After hours access

Common Types of Physical Security Breaches

Simplex 5 button lock

- Simplex claims that "thousands of combinations are available," in truth only 1081 combinations are used. Simplex advises against their use, and in most cases, does not even inform the user that these codes are available.
- Another 1081 combinations are available in the guise of "high security half-step codes
- Simplex advises against their use, and in most cases, does not even inform the user that these codes are available.
- **Vast majority of locks use default 1,2,3,4.**

Common Types of Physical Security Breaches

Swipe card access is a great way to secure a building or rooms housing sensitive equipment like data centres or server rooms.

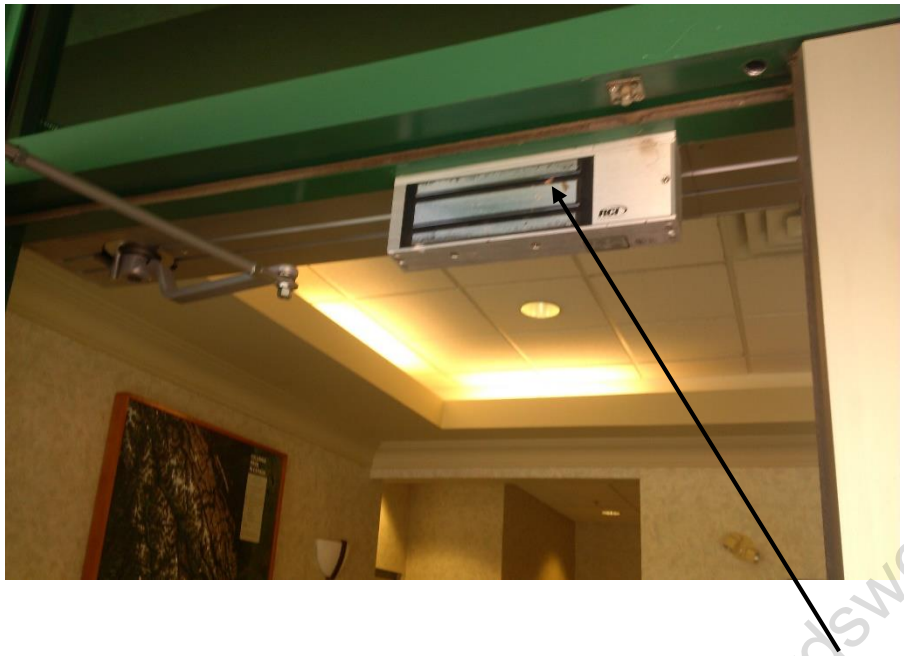
- A swipe card security system replaces traditional keys and locks with an electronic swipe card and reader.

- What is unique about card access systems is the ability to individually program each user's key card. This gives owners the chance to grant several levels of security clearance to employees and clients.

Additionally, card access systems allow for logging of entry and exit, so you know who has gone in and out, plus will notify of unauthorized access events.

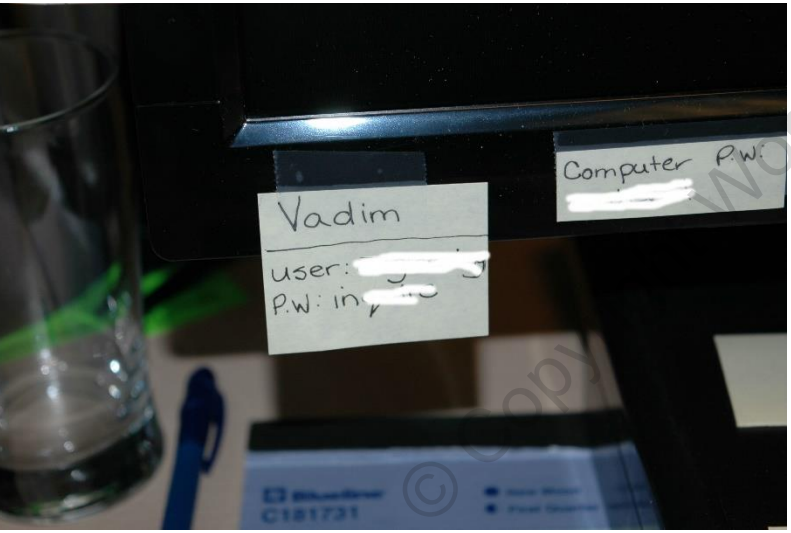
Except: …….

Common Types of Physical Security Breaches



Common electromagnetic lock easily defeated by attaching a metal sheet along the magnet to reduce the degree of magnetic force on the lock. If undetected, the door may be opened with little or no magnetic resistance.

Common Types of Physical Security Breaches



Common Types of Data Security Breaches - Internal

Result:
You are PWND!!

Common Types of Data Security Breaches

Only by understanding all the types of breaches your company is at risk of and how to defend against these can you achieve effective security and adequately mitigate your risk of breaches.

Authentication 101

Pet Peeve – Passwords

Authentication 101

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.

-WhatIs.com

Authentication 101

Authentication 101

Types:

The most frequent types of authentication available in use for authenticating online users differ in the level of security provided by combining factors from the one or more of the three categories of factors for authentication:

Single-factor authentication:

As the weakest level of authentication, only a single component from one of the three categories of factors is used to authenticate an individual's identity. The use of only one factor does not offer much protection from misuse or malicious intrusion. ***This type of authentication is not recommended for financial or personally relevant transactions that warrant a higher level of security.***

Authentication 101

Two-factor authentication

When elements representing two factors are required for authentication, the term two-factor authentication is applied — e.g. a bankcard (something the user has) and a PIN (something the user knows).

A good example from everyday life is the withdrawing of money from a cash machine; only the correct combination of a bank card (something that the user possesses) and a PIN (personal identification number, something that the user knows) allows the transaction to be carried out.

Authentication 101

Multi-factor authentication

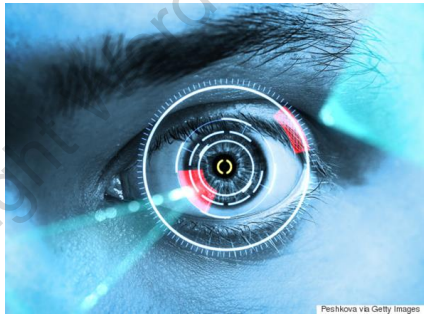
Multifactor authentication combines two or more independent credentials: what the user knows (password), what the user has (security token) and what the user is (biometric verification).

The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database.

If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.

Authentication 101

Types of MFA Technologies



MFA Options

Key Fobs:

- One-time password generators that come in the shape of key fobs with a small LCD screen came into vogue during the early days of multifactor authentication more than a decade ago.
- The screen on the key fob displays a sequence of numbers for 30 seconds.
- The user must then accurately type this sequence during that time period into the application or resource they are attempting to access.
- The passcodes generated by key fobs are checked against a server located on the enterprise network to ensure that they match. This server runs the identity management processes, sets up various security policies and connects the tokens with user directory stores such as Active Directory or RADIUS.

MFA Options

Smart Phones:

- Various smartphone apps have been built to generate the same one-time passwords as key fobs, and can help alleviate the above issues.

- And, as manufacturers add fingerprint sensors to their phones, the second factor can move beyond simple one-time numeric passwords to recognizing a digital copy of a user's fingerprint from a smartphone's built-in scanner.

MFA Options

Facial recognition:

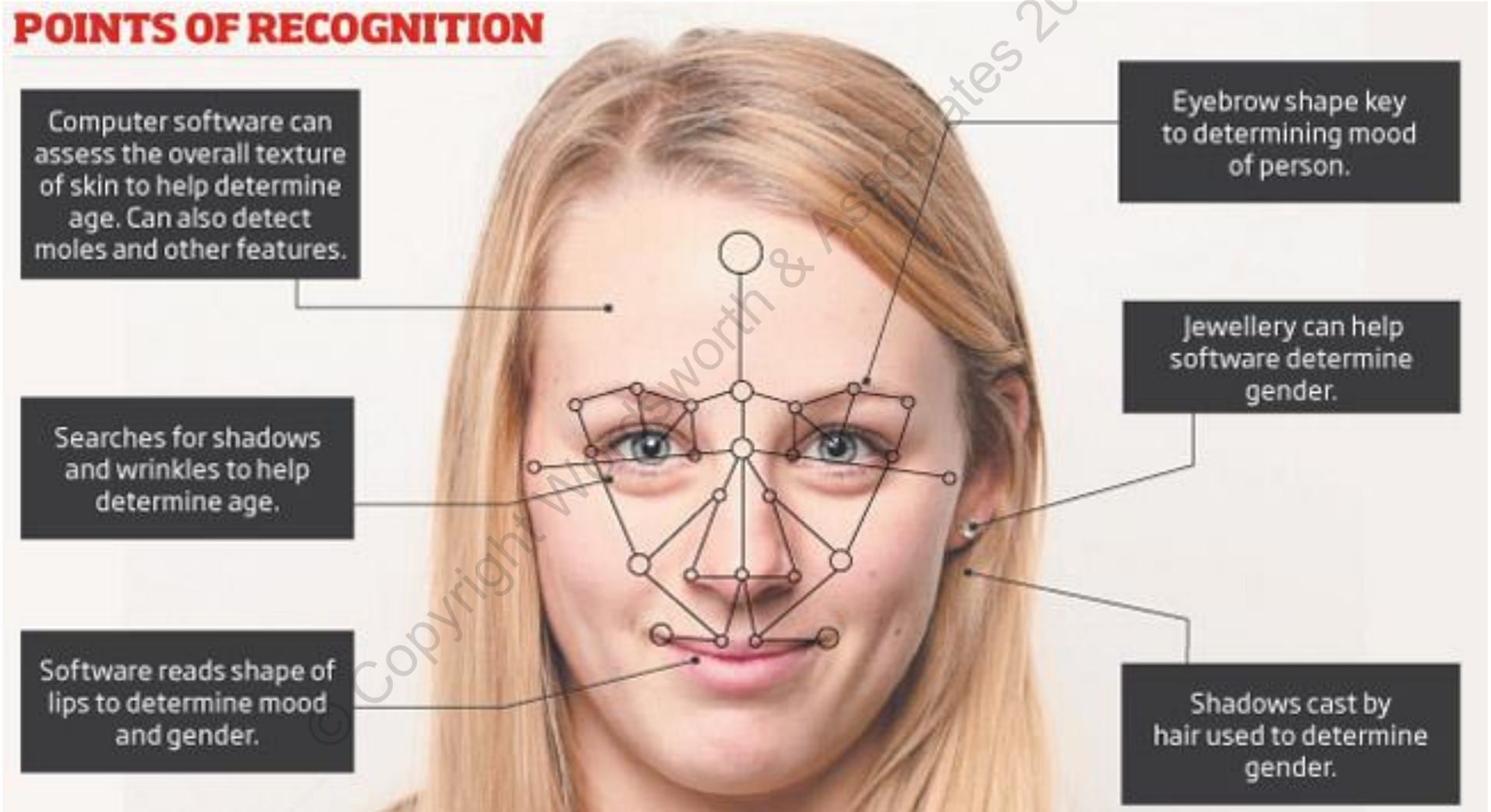
- A face recognition system is a computer application capable of identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a face database.

- It is typically used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems.

- Some face recognition algorithms identify facial features by extracting landmarks, or features, from an image of the subject's face. For example, an algorithm may analyze the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw.

MFA Options

Facial recognition:



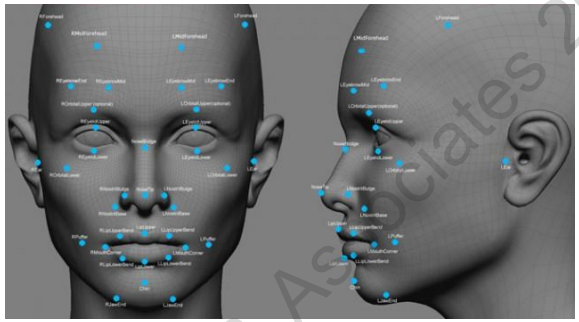
MFA Options

Who uses facial recognition technology?

Casinos use it to help identify crooks & addictive gamblers

Dating sites match people with the same facial features - uses the theory that people are most attracted to those that look like them.

Law enforcement and security use it to track down criminals - The FBI and Homeland Security have been able to use this for a long time to identify threats.



Credit card companies will allow you to shop with your face - MasterCard is researching ways to let their customers pay for things using a selfie, which prevents fraud and identity theft, and you don't have to remember passwords or put your credit card information on the web.

Social Media can tag people automatically - Facebook and its 140 billion photos of 600 million users uses Facial Recognition to identify everyone.

Upscale hotels greet guests upon arrival

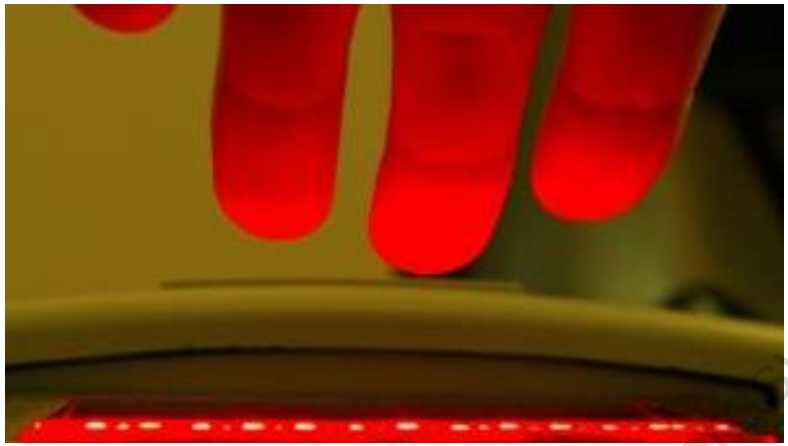
MFA Options

What other authentication technologies are being considering?

- Nymi, a Toronto-based startup that created a wristband that can identify its wearer based on their electrocardiogram, or the electrical activity of their heart, completed successful pilot projects alongside RBC and TD Bank to test out how its wristband can be used to verify purchases.

MFA Options

What other authentication technologies are Banks considering?



The popularity of the iPhone's fingerprint scanner has made consumers more comfortable and familiar with biometrics, according to a MasterCard executive

MFA Options

What other authentication technologies are Banks considering?

Iris & Retinal Scanning

Royal Bank is currently testing out technologies such as iris scanning, face recognition, speech recognition and fingerprint scans — and is expecting to roll out the features to customers in 2017.

MFA Options

What other authentication technologies are being considering?

Voice Recognition Technology

Barclays Bank rolls out voice recognition security - All clients of Barclays bank will now be able to verify their banking accounts using voice-recognition technology

A user's voice will now be accepted as verification to gain access to a bank account via telephone, replacing the keying in of a password. The service had been offered to premium account holders of the London-based financial services provider, but is now being made available to all 48 million clients worldwide.

MFA Options

What other authentication technologies are being considering?

Behavior detection

Biometrics can also identify users based on how they behave — for instance, their typing patterns or the way that they swipe across the screen on a mobile device **(or the way they are waving their gun)!**

MFA Options

What is coming in the future?

Rectal recognition software launched! Yeah!

- AnaLogics, a company based in New Jersey, is a developer of rectal recognition technology
- Rectal recognition software is based on the ability to first recognize rectums, which is a technological feat in itself, and then measure the various features of each rectum.
- The rectum has certain distinguishable landmarks. AnaLogics defines these landmarks as nodal points.
  - There are about 80 nodal points on a human rectum. Nodal points that are measured by the software: distance between buttocks, width of perineum, contour of sphincter, gluteal mass, presence of hemorrhoids.

MFA Options

The basic process that is used by the Rectognize system to capture and compare images:

Detection - When the system is attached to a video surveillance system, the recognition software searches the field of view of a video camera for rectums.

Alignment - Once a rectum is detected, the system determines the anus position, size and pose.

Normalization -The image of the rectum is scaled and rotated so that it can be registered and mapped into an appropriate size and pose.

Representation - The system translates the rectal data into a unique code.

Matching - The newly acquired rectal data is compared to the stored data and (ideally) linked to at least one stored rectal representation.

The heart of the Rectognize rectal recognition system is the Excretory Feature Analysis (EFA) algorithm. This is the mathematical technique the system uses to encode rectums.

Interesting Breaches

Canada Revenue Agency

March 2017 - Shared Services Canada says IT security staffers were made aware of a bug in a computer program widely used by the federal government. But it took until Thursday, after a breach was discovered at Statistics Canada, that the plug wasn't pulled on the agency's web servers for 24 hours.

Interesting Breaches

CloudPets

In 2016, more than 727,000 UK children had their information compromised following a cyberattack on VTech. Now, another internet connected range of children's toys has been found to be exposing the personal details of children.

CloudPets, the maker of Internet of Things teddy bears, left more than two million voice recordings from children online without any security protections. Ars Technica reported the company had been contacted about the vulnerability multiple times but had not responded.

Freedom Hosting II

The web host has details on around 20 per cent of all sites on the dark web. In February, 2017 the firm was hit by a hacker who swiped the company's database of customers.

In total, 74GB of data stored on servers was reportedly taken, with some of this being child pornography. As well as the files, a 2.3GB database of customer information was also taken. 381,000 email addresses were included in the MySQL database. It is said the data included "thousands" of .gov email addresses.

Now defunct!

PlayStation and Xbox forums

More than 2.5 million gamers that use the XBOX360 ISO and PlayStation's PSP ISO forums had their account details compromised. The details taken include email addresses, passwords and IP addresses.

The data breach happened in 2015 but has only just been found and made public. PSP ISO had 1.3m account details taken and Xbox360 ISO had 1.2m accounts hit.

Cloudflare

Personal messages sent on dating websites, Uber trips, and more were all leaked online after a problem with internet company Cloudfare's software. A bug in the software, which is used by millions of websites, meant that unhashed and plaintext information was being published to the web between September 2016 and February 2017.

While technically not a hack, the passwords and sensitive personal information of customers who use the websites affected were cached by search engines after they were published online. It is not known how much personal data was leaked in the incident that has been dubbed Cloudbleed.

Recent Breaches

Canadian Tire

Five days after it suspended customer login access to its retail website, which allows consumers to track their loyalty accounts, Canadian Tire Corporation admited customer information may have been stolen.

An unknown third party may have obtained customer log-in information, including their email address and password information, from a prominent third-party website breach and used this information to gain access to canadiantire.ca accounts.

Goldcorp

2016 - Hackers hacked Goldcorp, a gold-mining firm with headquarters in Vancouver, British Columbia, and dumped a trove of private company and employee data online.

In a document posted to a public paste site, the hackers provided sample data and a link to a full torrent download, which measured 14.8 GB when uncompressed.

The sample data includes what appears to be correspondence to some employees concerning their 2013 performance and 2014 compensation rates, proprietary information, bank account information (not dated), budget information for 2016, international contacts, and directories of employees by location with their names, titles, office, and mobile telephone numbers and email addresses.

Preparing for the Inevitable Privacy and Security Incident

Educate employees in security awareness:

Security awareness is the knowledge and attitude members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization.

Phishing attacks are **the** most common security challenges that both individuals and companies face in keeping their information secure. Whether it's getting access to passwords, credit cards, or other sensitive information, hackers are using email, social media, phone calls, and any form of communication they can to steal valuable data. Businesses, of course, are a particularly worthwhile target.

Oh @#$%^! Now what?

Depends:

- **If you are confident in your backup integrity:**
  - Options – pull plug on Internet
  - Pull plug on server
  - Re-image device
  - Restore applications & data

- **If you are <u>not</u> confident in your backup integrity:**
  - Consider paying the ransom
  - Negotiate with hacker
  - Consider setting up bitcoin account – Be prepared
  - Throw yourself in the nearest river!

- **Hope & Pray!**

Oh @#$%^! Now what?

- **Review what Personal Identifiable Information (PII) has been extracted:**

  - ✓ Customer information
  - ✓ Credit Card information
  - ✓ Employee information
  - ✓ etc.

- **Be transparent – notify affected parties**

  - ✓ Customers
  - ✓ Insurance Companies
  - ✓ Banks
  - ✓ Privacy Commissioner – Compulsory Breach notification soon!

Oh @#$%^! Now what?

Should I contact Law Enforcement?

Probably not – Unlikely they can help!

The following three pillars are identified within the strategy to guide the RCMP's efforts in combating cybercrime:

- Identify and prioritize cybercrime threats through intelligence collection and analysis;
- Pursue cybercrime through targeted enforcement and investigative action; and,
- Support cybercrime investigations with specialized skills, tools and training.

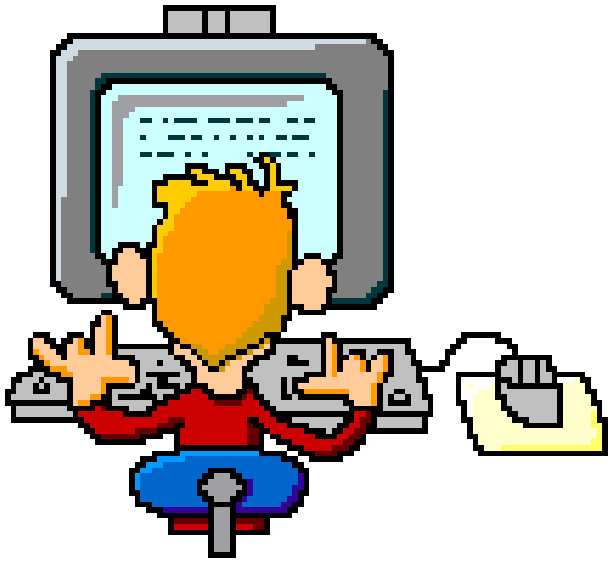
Priorities are:

Child protection
Terrorism
Threat of life
Threat of Life
Homicide

Lessons Learned

- Complete an independent network security review
- Ensure your backup is not on your network
- Take a backup off-site
- Regularly confirm the integrity of your backup
- Provide employee security awareness training
  - Develop employee policies
  - Promote strong password policies
- Develop a business continuity & disaster recovery plan
- Develop security incident response plan

Thank You!



QUESTIONS?

Wordsworth & Associates

(604) 535 7213

charles@netsafe.ca

www.wordsworthandassociates.com