

# CitA TECH LIVE

Let's Talk Digital!



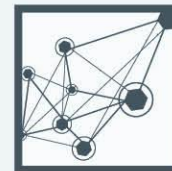
**CitA TechLive:**  
**Showcasing**  
**construction**  
**technologies**

Croke Park, November 8th & 9th 2018

# CitA | TECH LIVE

Let's Talk Digital!

# Welcome



Showcasing construction technologies

Croke Park, November 8th & 9th 2018

**CitA** | **TECH**  
**LIVE** Let's Talk Digital!

# Keynote

## Cyber Threat Landscape & Risk Mitigation



**Brian Casserly**  
**Cyber Security Analyst**





## Cyber Threats Actors

**Cybercriminals**



**Nation States**



**Hacktivists**



**Corporate Espionage**



**Insider Threat**



**Terrorism**









## Cyber Threats Examples



FORA THE 42 THE DAILYEDGE

Irish Politics International Voices Family Culture Tech Business My Feed

Tags # AMSTERDAM # BITCOIN # CARTEL # CRYPTOCURRENCY # DRUGS # KINAHAN

### European police target Kinahan's hidden Bitcoin cash in Belgium and the Czech Republic

A Bitcoin 'mine' was discovered in a raid on the cartel last month.

23 hours ago 38,321 Views 60 Comments

Share 142 Tweet Email 6

MILLIONS OF EURO is being washed through online currencies and European banks by accountants and Belgian Bitcoin experts who are being paid by the Ireland's biggest gangs.

Gardaí and international police have long suspected that the Kinahan drug gang had been washing its money through online currencies such as Bitcoin. However, last month's arrest of a number of suspected drug traffickers in the Netherlands brought with it the seizure of what is known as a bitcoin mining rig.



Image: Shutterstock/PORTRAIT IMAGES ASIA BY NONWARIT

### What Happened?



On Saturday, June 23, 2018, Ticketmaster UK identified malicious software on a customer support product hosted by Inbenta Technologies, an external third-party supplier to Ticketmaster.

As soon as we discovered the malicious software, we disabled the Inbenta product across all Ticketmaster websites.

Less than 5% of our global customer base has been affected by this incident. Customers in North America have not been affected.

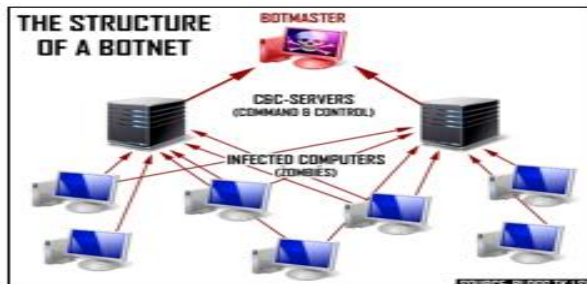
As a result of Inbenta's product running on Ticketmaster International websites, some of our customers' personal or payment information may have been accessed by an unknown third-party.

We have contacted customers who may have been affected by the security incident. UK customers who purchased, or attempted to purchase, tickets between February and June 23, 2018 may be affected as well as international customers who purchased, or attempted to purchase, tickets between September 2017 and June 23, 2018.

**If you have not received an email, we do not believe you have been affected by this security incident based on our investigations.**

Forensic teams and security experts are working around the clock to understand how the data was compromised.

We are working with relevant authorities, as well as credit card companies and banks.



## MALWARE

**Malware derives from Malicious Software**

**Malware is distributed by Cybercriminals with the intent of *stealing, corrupting or destroying* data on devices & networks.**

**Malware comes in a variety of forms but all of them try to exploit your data in some way**







## KEYLOGGER



 **WARNING!**  
Wireless keylogger Hidden inside USB Charger  
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

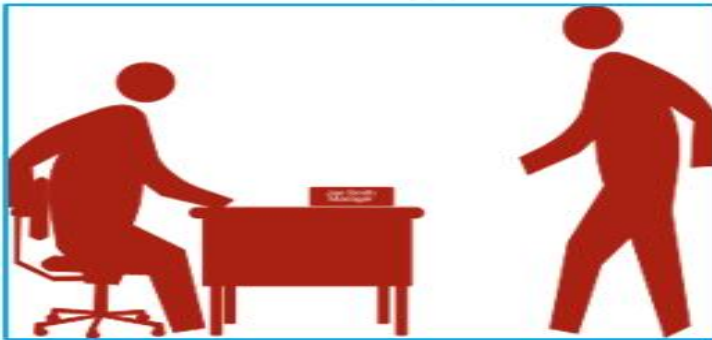






## Social Engineering

**Pre-Texting**



**Impersonation**



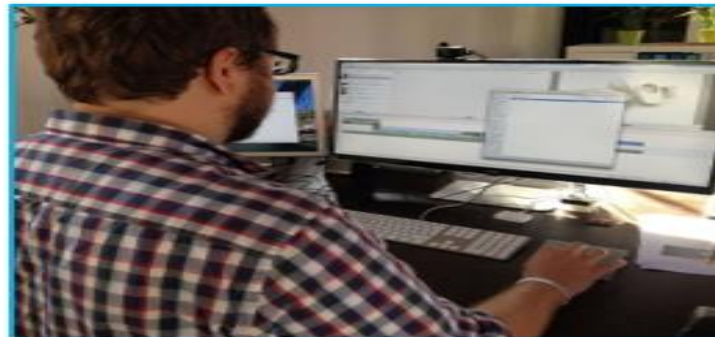
**Honey Traps**



**Tail-gaiting**



**Shoulder Surfing**

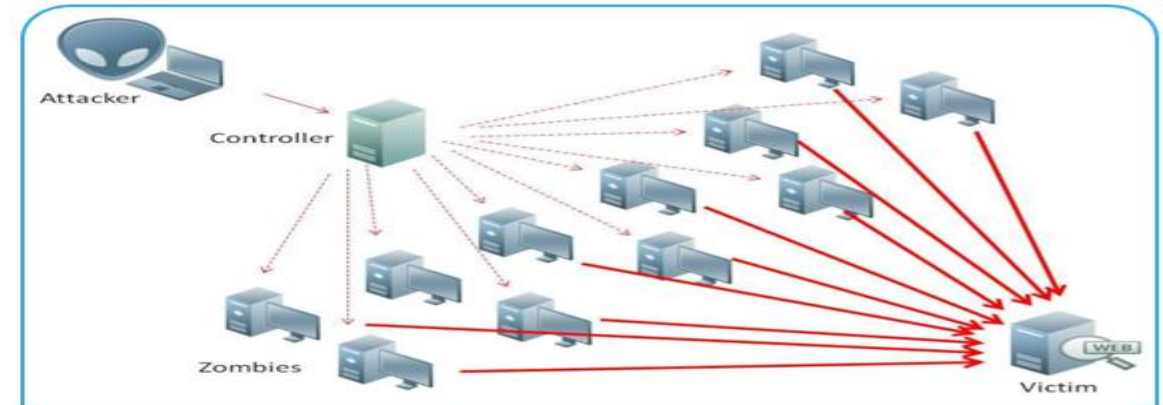
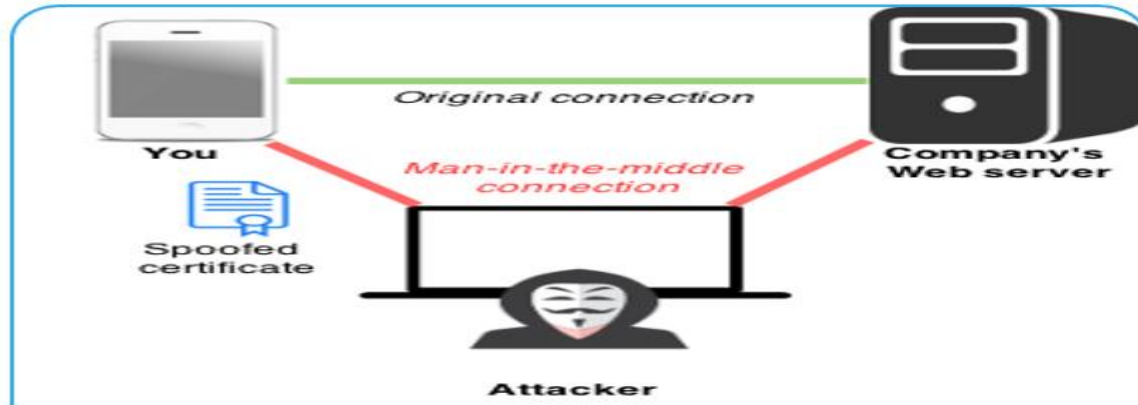


**Dumpster Diving**





## Common Cyber Attacks



```
key no. 9080000: UNTP4RT22
key no. 9090000: UNTPUD2D2
key no. 9100000: UNTPPPUU2
key no. 9110000: UNTR442P2

The PSK is "UNTR4P2ND".

9112546 passphrases tested in 48.53 seconds: 187769.14 passphrases/second
root@kali:~/Desktop# aircap-ng -e cheekymonkey -p UNTR4P2ND A2-01.cap
Total number of packets read      39289
Total number of WEP data packets    0
Total number of WPA data packets  14613
Number of plaintext data packets    0
Number of decrypted WEP packets     0
Number of corrupted WEP packets     0
Number of decrypted WPA packets    14404
```





## Business E-Mail Compromise

Cyber-Enabled Financial Fraud on the Rise Globally

### Step 1: Identify a Target



Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

### Step 2: Grooming



Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).

Perpetrators use persuasion and pressure to manipulate and exploit human nature.

Grooming may occur over a few days or weeks.

### Step 3: Exchange of Information



The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

### Step 4: Wire Transfer



Upon transfer, the funds are steered to a bank account controlled by the organized crime group.\*

\*Note: Perpetrators may continue to groom the victim into transferring more funds.

## Business E-Mail Compromise Timeline

An outline of how the business e-mail compromise is executed by some organized crime groups



## Business E-Mail Compromise cont.



In the latest bogus email scam in the county, a businessman's payment for construction work on his premises was redirected at the last minute by scammers who hoodwinked the company out of €70,000.

Gardaí managed to recover half of the money before it left the country and investigations are ongoing.





## Business E-Mail Compromise cont.

Tags: # CEO FRAUD # CRIME # MEATH # MEATH COUNTY COUNCIL # THOMAS EYRE

### €4.3 million mistakenly transferred by Meath County Council frozen in Hong Kong bank

A criminal investigation is underway into the stolen money, which has been secured in a Hong Kong bank.

Dec 19th 2016, 3:36 PM 16,133 Views 24 Comments

MEATH COUNTY COUNCIL has confirmed that the €4.3 million stolen in a bogus email scam is now frozen in a bank account in Hong Kong.

In recent weeks, the council was the subject of a "CEO fraud" scam, whereby emails purporting to be from council chief executive Jackie Maguire asked for the transfer of the funds.

The council's bank was alerted to the fraud, and the theft was detected before it was completed. A criminal investigation is underway into the scam.

Fianna Fáil Meath East TD Thomas Eyre said the council should not be jeopardised by the temporary nature of their own cyber security procedures.

In a statement today, the council said it had taken legal proceedings to recover the stolen €4.309 million. It added:

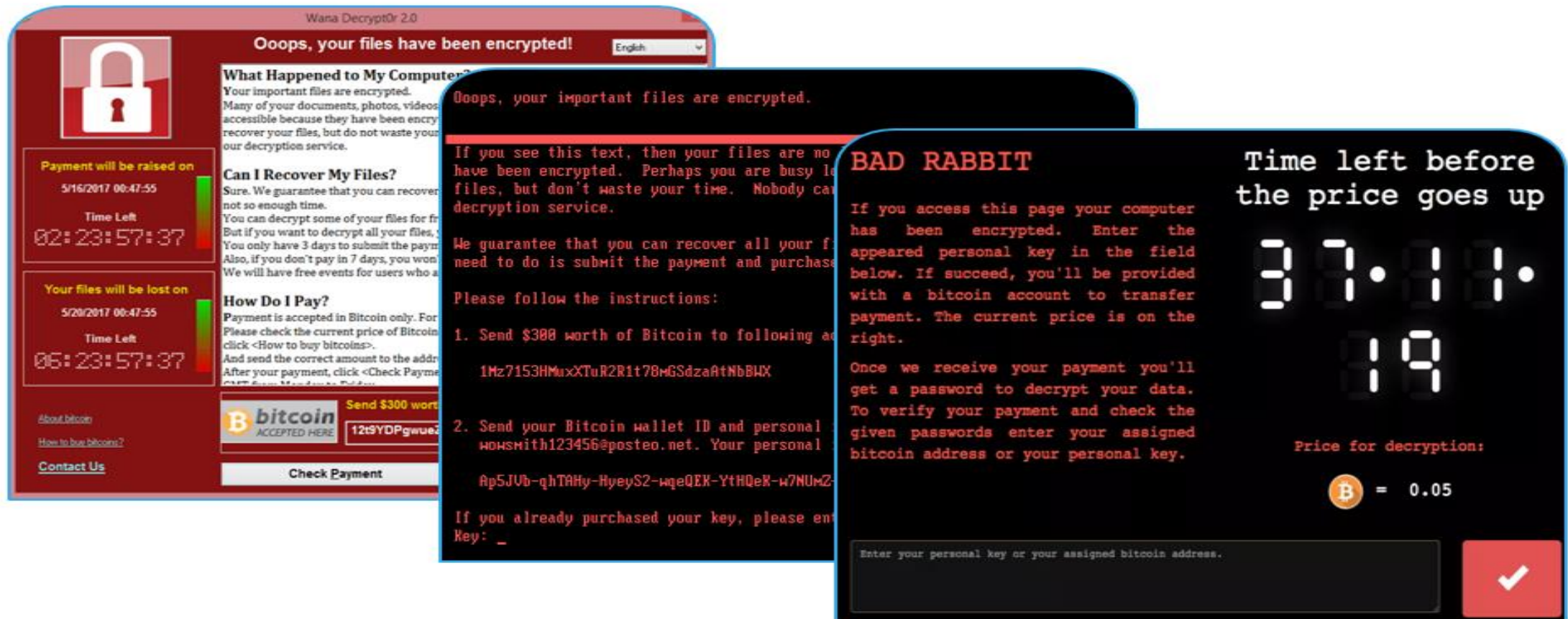
Meath County Council has confirmed that it has taken legal proceedings in Hong Kong and that the funds have been secured on foot of a court order obtained by Meath County Council.

In a statement today, the council said it had taken legal proceedings to recover the stolen €4.309 million. It added:

Meath County Council has confirmed that it has taken legal proceedings in Hong Kong and that the funds have been secured on foot of a court order obtained by Meath County Council.



## Ransomware



**Wana Decrypt0r 2.0**  
Oops, your files have been encrypted!

**What Happened to My Computer?**  
Your important files are encrypted. Many of your documents, photos, videos are inaccessible because they have been encrypted. We can recover your files, but do not waste your time on our decryption service.

**Can I Recover My Files?**  
Sure. We guarantee that you can recover your files, but not so enough time. You can decrypt some of your files for free. But if you want to decrypt all your files, you only have 3 days to submit the payment. Also, if you don't pay in 7 days, you won't get your files back. We will have free events for users who are affected.

**How Do I Pay?**  
Payment is accepted in Bitcoin only. For payment, please check the current price of Bitcoin and click <How to buy bitcoins>. And send the correct amount to the address. After your payment, click <Check Payment>.

**Payment will be raised on**  
5/16/2017 00:47:55  
Time Left  
02:23:57:37

**Your files will be lost on**  
5/20/2017 00:47:55  
Time Left  
06:23:57:37

**Send \$300 worth of Bitcoin**  
12t9YDPgwue2

**Check Payment**

**BAD RABBIT**  
If you see this text, then your files are not encrypted. Perhaps you are busy looking at your files, but don't waste your time. Nobody can help you with decryption service.

We guarantee that you can recover all your files. You need to do is submit the payment and purchase the decryption service.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:  
1Mz7153HMuXTuR2R1t78wGSdzaAtNbBWx
2. Send your Bitcoin wallet ID and personal key to: w0HSmith123456@posteo.net. Your personal key: Ap5JUv-qhTAHy-HyeyS2-wqeQEX-YtHQeK-w7NUM2

If you already purchased your key, please enter your key: \_

**Time left before the price goes up**  
37:11:19

**Price for decryption:**  
1 Bitcoin = 0.05

Enter your personal key or your assigned bitcoin address.





## Case Study



### PRESS RELEASE

July 03, 2017

#### CYBER-ATTACK UPDATE

Like several other companies Saint-Gobain experienced an important cyber-attack on June 27, 2017. IT systems were disconnected to stop the spread of the virus and back-up working modes were immediately activated in all businesses of Saint-Gobain. No personal data has been disclosed to any third party.

Throughout the event all efforts have been made to ensure the continuity of our business and in particular to keep any impact on our customers to a minimum. The majority of our businesses are already operating normally. One week after the attack, substantial progress has been made to put all of our systems back on line with a full return to normal operations expected early next week.

#### ABOUT SAINT-GOBAIN

Saint-Gobain designs, manufactures and distributes materials and solutions which are key ingredients in the wellbeing of each of us and the future of all. They can be found everywhere in our living places and our daily life: in buildings, transportation, infrastructure and in many industrial applications. They provide comfort, performance and safety while addressing the challenges of sustainable construction, resource efficiency and climate change.

€39.1 billion in sales in 2016  
Operates in 67 countries  
More than 170,000 employees  
[www.saint-gobain.com](http://www.saint-gobain.com)  
[@saintgobain](https://twitter.com/saintgobain)

 News • Somerset News • Twitter

## Jewson builder's merchants, with 11 Somerset branches, hit by worldwide cyber attack

The 'Petya' cyber attack originated in Ukraine but has rapidly spread across the world

By  Reporter  
17:38, 28 JUN 2017



The firm has branches in Yeovil, Chard, Taunton, Bridgwater (above), Highbridge, Weston-super-Mare, Clevedon, Bath, Radstock, and two in Frome.

#### RECOMMENDED



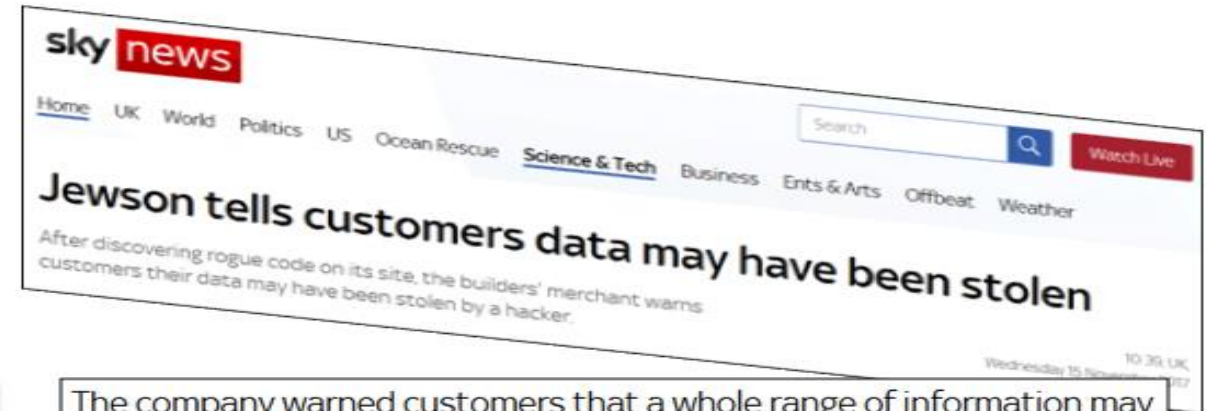
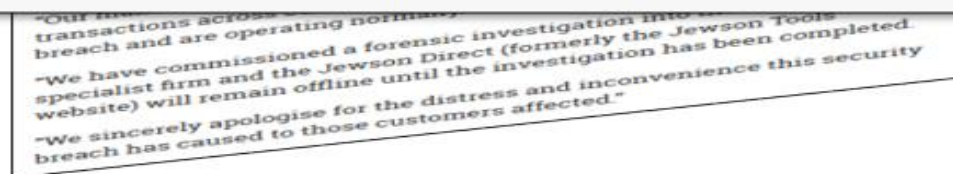


## Case Study



Affecting the Jewson Direct website only, the breach was discovered on 3 November 2017 and Jewson has been in touch with 1,659 customers who may have been affected.

The Saint Gobain-owned business has over 600 branches across the UK.



The company warned customers that a whole range of information may have been stolen during the breach.

Names, location, billing address, password, email, phone number, payment details, card expiry dates and CVV numbers "may" have fallen into the hands of an "unauthorised person", according to the report.

"At this stage we are aware that a foreign piece of code was encrypted into the Jewson Direct (formerly Jewson Tools Direct) website," the company told customers.





## Future Threats?



### Exploring the Potential for Autonomy

5G will be crucial in providing the infrastructure we need to develop autonomous machines. In essence, this new generation of mobile network is expected to deliver transfer speeds considerably faster than the current 4G network, and is therefore capable of transporting huge amounts of data in far less time. This will mean self-driving construction machines will be able to recognize signals, map an area more accurately, and communicate with each other far more easily than ever before. All of this will make construction sites run more efficiently and safely.

In sectors such as mining, where it can take several hours of ventilation after blasting rocks before the environment is safe enough for operators to enter, moving closer to removing humans from the production site entirely will bring great advantages in productivity and safety.

Drone technology will also receive a boost. Increased bandwidth, coupled with reduced latency and improved reliability, will allow a seamless transfer of ultra-high-definition video. And while virtual reality has been slow to take off, partly due to a lack of connectivity issues, the increased efficiency of 5G could unlock its true potential.



# ILLUMINATE

## LEARNING





## **Common Sense Approach**

- 1. Back Up Data regularly**
  - i. 3-2-1 Rule

- 2. Use Strong Passwords**
  - i. The longer; the better.
  - ii. No pets, No kids, No partners

- 3. Don't Share Passwords**
  - i. Don't Share Accounts
  - ii. Don't write Passwords down

- 4. Get Anti-Virus**
  - i. Malwarebytes
  - ii. Scan USBs & Ext. HDs
  - iii. AV for Mobile Devices

- 5. Scan devices regularly**
  - i. Set a time to do a full scan
  - ii. Know what a detection looks like
  - iii. Don't ignore alerts

- 6. Secure devices Physically & Electronically**
  - i. PINs, Patterns & Biometrics
  - ii. Locks & Chains

- 7. Be cautious with e-mail**
  - i. Check with sender
  - ii. Scan attachments
  - iii. Check links are legitimate

- 8. Limit Social Media information**
  - i. Restrict "Friends"
  - ii. Limit location info
  - iii. Secure accounts

- 9. Use HTTPS everywhere**
  - i. Especially with financial transactions
  - ii. Bookmark websites

- 10. If in doubt get a 2nd opinion**
  - i. 'There are no stupid questions'
  - ii. Google search



## C-Suite

### SECURITY CORPORATE CULTURE

Identifying business assets, whether that's people, technology, intellectual property or physical property creates the blueprint for appropriate security measures. Our team will identify if the C-suites view on security is in line with best practice security risk management levels.

## Physical

### DEFENCE IN DEPTH

This is a process of identifying the layers of physical security in situ that can decrease your risk of threat. Vulnerabilities in your physical security offers an open door to those wishing to exploit your team, your technical measures and your business stability.

## Technical

### CYBER SECURITY MEASURES

Our team will conduct a Web Application Vulnerability Scan on your website, Wifi Access Audit, conduct open source information gathering on the business followed by Phishing simulations. Finally, we will perform access injection techniques (if feasible) to provide your business with a snapshot of your cyber security landscape in conjunction with our physical and team assessments.

## People

### INTERNAL & EXTERNAL

It is widely acknowledged that the human barrier to security can often be an organisations greatest asset and weakness. Our HRA reviews the employee's security sentiment, 3rd party contractors accessibility, and potential exploitation of social engineering.



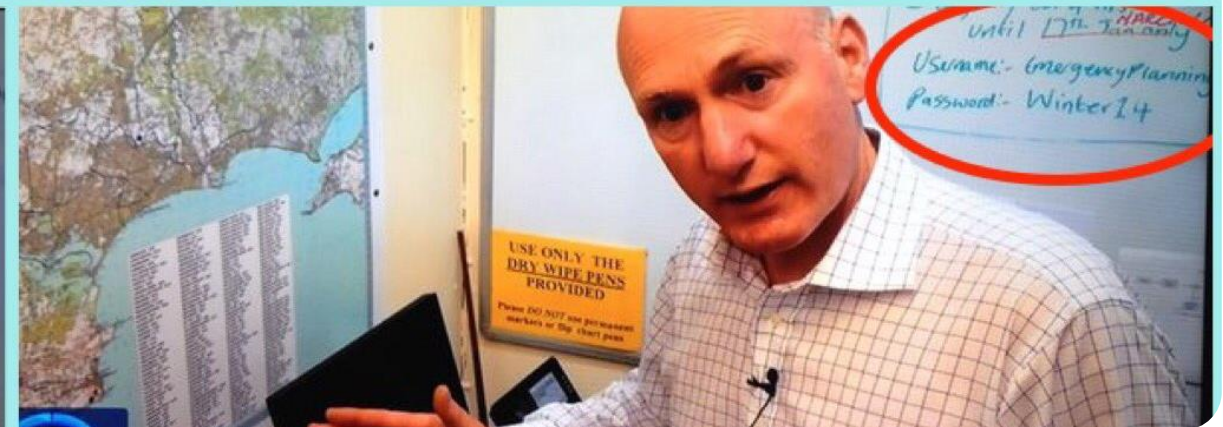
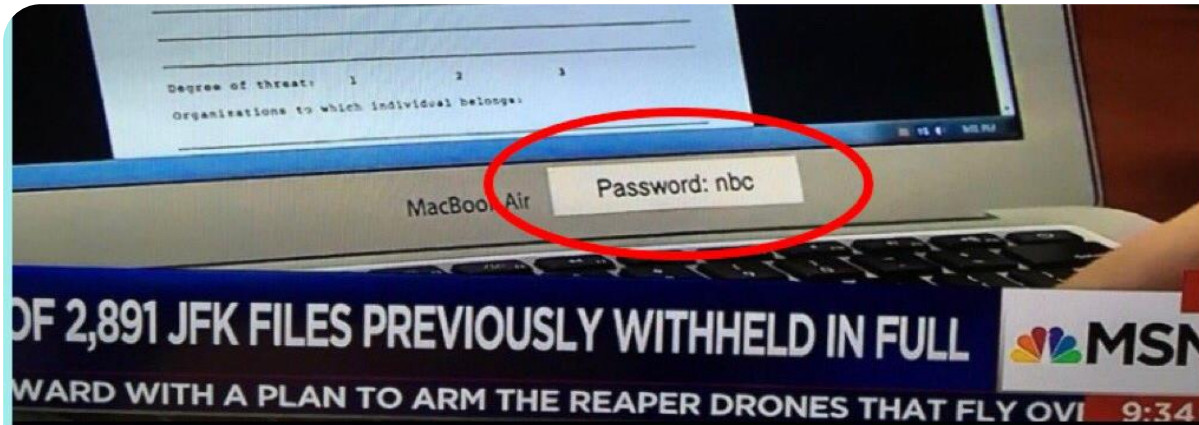
**RESILIENT  
DEFENCE**

[www.resilientdefence.com](http://www.resilientdefence.com)





Finally...



**CitA** | **TECH**  
**LIVE** Let's Talk Digital!

**Thank you**

**Brian Casserly**  
**Cyber Security Analyst**



**RESILIENT**  
DEFENCE