

CYBER BREACH NOT IF, BUT WHEN

AIRMIC Conference Workshop, 12 June 2017

JOIN THE DISCUSSION

Go to: [slido.com](https://www.slido.com)

Enter Code: HDI2017

This document contains – if not already published in financial statements, annual or quarterly reports – confidential and sensitive information/business secrets regarding the insurance business or certain relations of the Talanx Group.

As the intended addressee of this information you are obligated – not only by labour regulations but also by regulatory laws (in this case also subject to penalty) – to keep this information strictly confidential, both within the company and particularly in relation to third parties.

We herewith duly inform you of this matter, even though we believe that for you as an employee of the Talanx Group the responsible and confidential handling of sensitive information would go without saying.

In case of any further questions regarding specific details, please do not hesitate to contact the Group Legal Department in Hannover.

Get Involved!

Go to: [slido.com](https://www.slido.com)

Enter Code: HDI2017

***“But, nobody wants what I
have...”***





This recent undated satellite image provided by Space Imaging/Inta SpaceTurk shows the once-secret Natanz nuclear complex in Natanz, Iran, about 150 miles south of Tehran.  AP Photo/Space Imaging/Inta SpaceTurk, HO

Sony Hack October 2011: Thousands Of PlayStation Network Accounts Targeted By Massive Attack

AP | By TOMOKO A. HOSAKA

Posted: 10/12/2011 9:05 am EDT | Updated: 12/12/2011 5:12 am EST





19 Online Cheating Site AshleyMadison Hacked

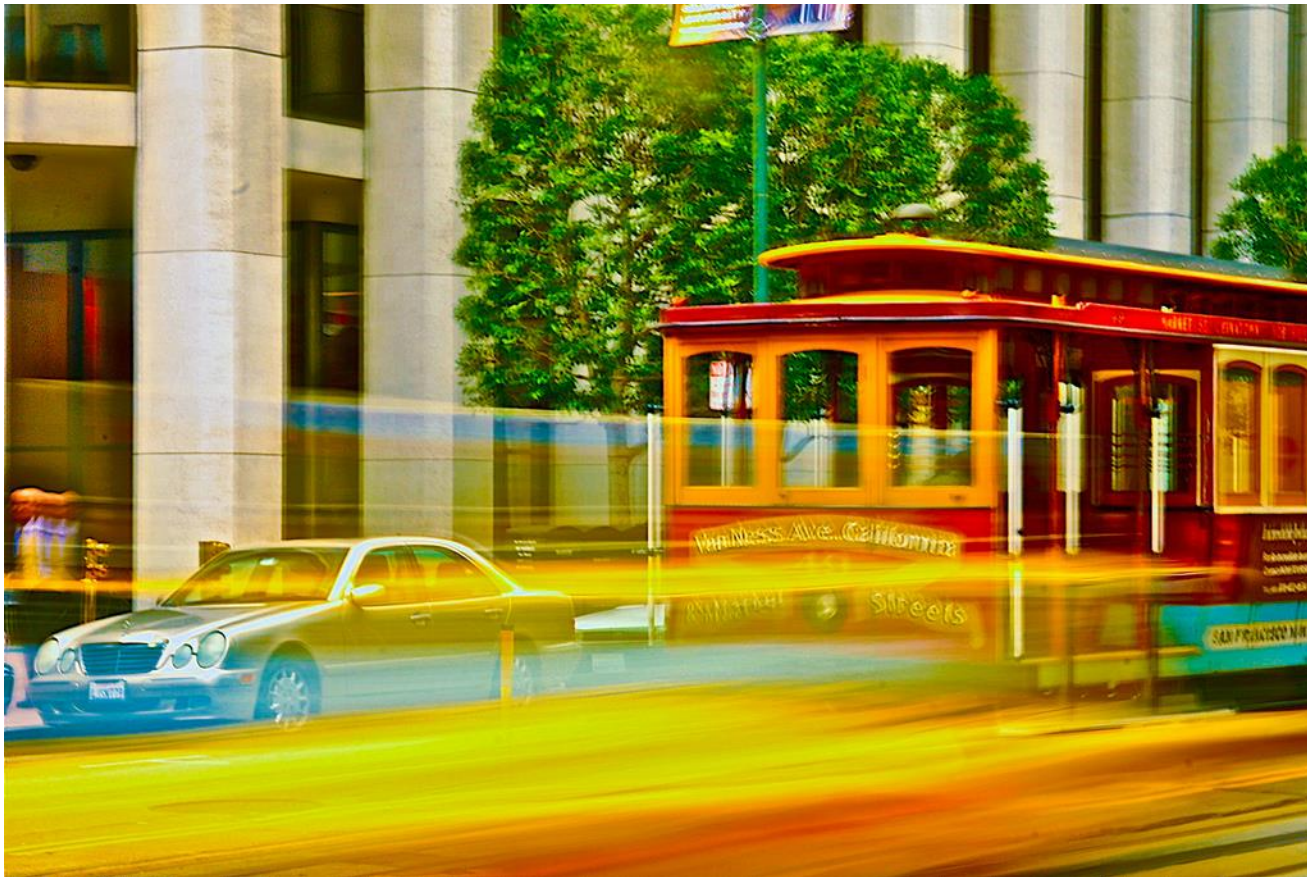
JUL 15



Large caches of data stolen from online cheating site **AshleyMadison.com** have been posted online by an individual or group that claims to have completely compromised the company's user databases, financial records and other proprietary information. The still-unfolding leak could be quite damaging to some 37 million users of the hookup service, whose slogan is "Life is short. Have an affair."



Cyber Breach – Not If, But When









REMINDER to Get Involved!

Go to: [slido.com](https://www.slido.com)


Enter Code: HDI2017

Peter Hawley

Cyber Underwriter

HDI Global SE - UK



- Peter Hawley
- Cyber Underwriter with responsibility for Cyber Insurance at HDI Global in the UK
- Member of the team who developed HDI Global's *Cyber+* product in London
- Worked in insurance for 14 years
- Founder committee member of the Cyber Insurance Association
-  @EC3Cyber



Nick Andrews

FCII, CFIRM, Chartered Insurance Risk Manager

Head of Insurance Risk

E D & F Man Holdings Limited



- Nick Andrews
- Head of Insurance Risk – E D & F Man Holdings Limited
- Manage a team of insurance and risk personnel to provide global insurance policies across marine and non-marine disciplines
- Worked in insurance for 30 years – Broker, Client, Insurer (underwriting and risk management)



Why?

- MAN Incidents.
- Third party incidents.
- Banks/Lenders interest.
- Everyone talking about it.
- Risk Committee asking - is a Private Company like MAN really at risk?

What did we do?

- Reviewed internal protections :
 - Safeguards limited.
 - Internal capability limited
- Buy-in from Main Board Director.
- 3 professional organisations tendered.
- Chose Source8 for deep down review.
- Ensure all divisions open for interviews.

Project overview

- Identify inherent cybersecurity risk by assessing complexity & business criticality of the technology.
- Evaluate maturity of current controls and effectiveness.
- Analyse likelihood & quantify impact.
- Produce rec's to align desired residual cyber risk with MAN's tolerance.

Recommendations

- Loss scenarios completed.
- 42 Rec's split 0-3, 3-6 & 6-12 months.
- Lot of low hanging fruit (password/m. sticks).

Actions


- New Cyber Employee.
- Cyber committee - board level.
- Monthly reviews and reporting of rec's.
- Risk & Insurance on Committee.

Stuart Peck

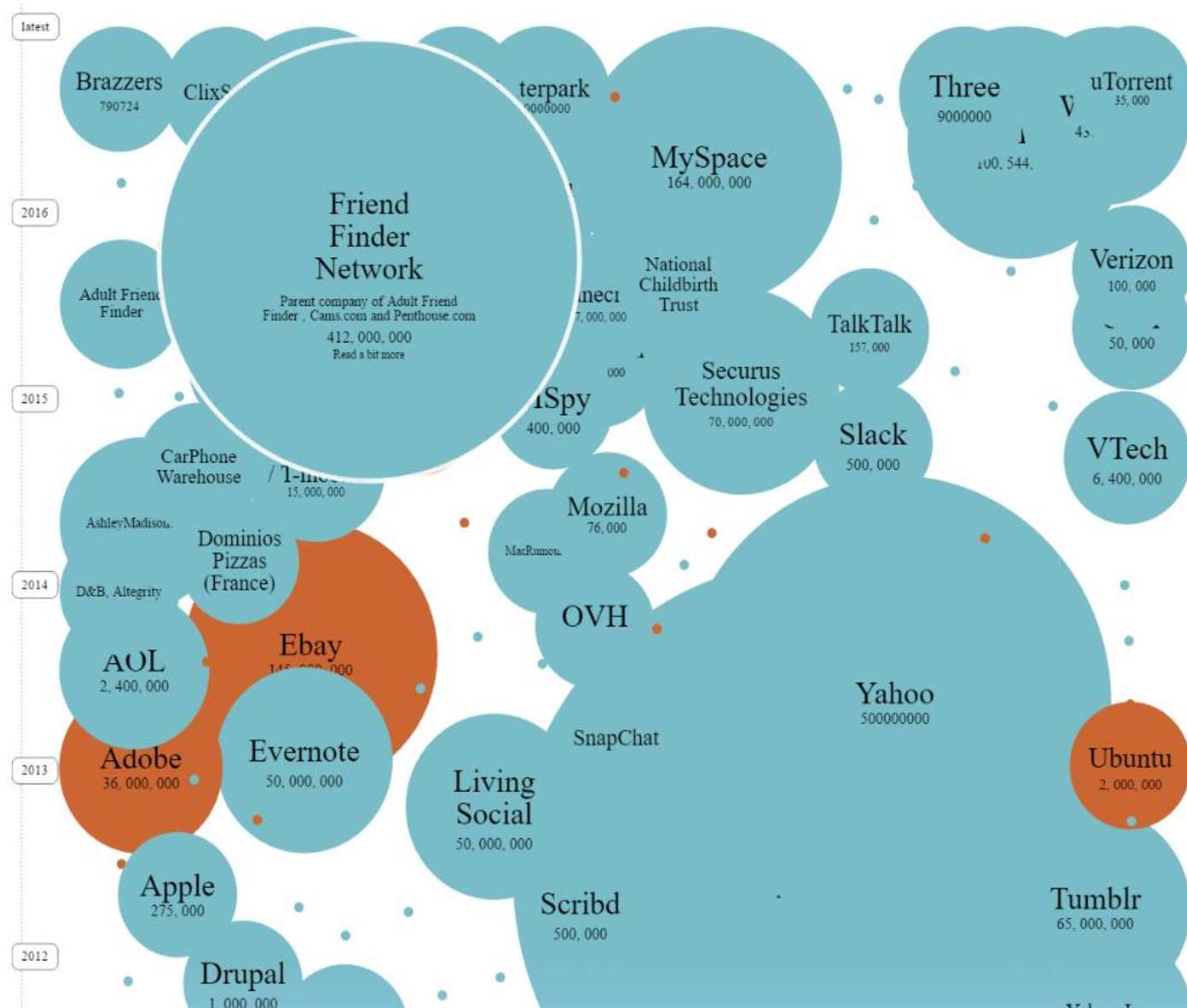
Head of Cyber Security Strategy

ZeroDayLab



- Stuart Peck
- Head of Cyber Security Strategy – responsible for Threat Intelligence, Research, and Education programs for ZeroDayLab globally
- Passionate about educating organisations and executives on the latest attacker trends facing businesses today and how to combat them
- 13 years industry experience in Information Security, known for being a subject matter expert on the Dark Web and Open Source Intelligence (OSINT)
- Creator of award winning “situational threat awareness” training program
-  @cybersecstu





The Cyber Security Specialist



1 Billion Records



419 Million Records



360 Million Records



164 Million Records



152 Million Records




85 Million Records



Threat Landscape... Dark Web

How much does information cost on the dark web?

There is a huge variety of stolen data for sale on the dark web, including both financial information and login details. It is also the place fraudsters go to buy the tools used to commit identity theft. Below, we look at the average price of various types of personal information for sale

Credit cards		Recent prices
 Visa Classic & Mastercard with user data		£28
		£28
		£11
 Visa Premium with user data		£35-42
		£35-42
		£21

Cyber Criminals use to commit more crime/fraud such as Vishing, or identity theft.

Cyber Criminals sell data on the dark web market place. The current going rate for 1 persons PII is \$200- or 0.14 in BitCoins

HXT IT

HXT service, elite hacking. Keep it simple, do it quick.

email: hxt@cock.li

Job	Price
Compromise facebook account*	\$120
Compromise email account*	\$175
Compromise online banking*	\$250
DDoS basic (1 week)	\$125
DDoS advanced (1 week)	\$250
Compromise vulnerable sites	\$250
500 Fresh botnet installs	\$500
Custom ransomware	\$700+
Our crypter service	\$50

PROFIT FROM PETYA & MISCHA!

HIGH INFECTION RATES

PETYA comes bundled with his little brother MISCHA. Since PETYA can't do his evil work without administrative privileges, MISCHA launches when those can't be obtained.

PETYA does a low level encryption of the disk, which is a completely new technique in ransomware. MISCHA acts as an traditional file-based ransomware. For more informations see our FAQ.

PROVABLY FAIR

As professional cybercriminals, we know that you can't trust anyone. So we developed a payment system based on multisig addresses, where no one (including us) can rip you off.

For more informations see our FAQ.

FREE CRYPTING SERVICE

We provide you FUD crypted binaries, and that 24/7. No need to buy shitty crypters or waste your money on expensive crypting services.

Additionally, for our distributors with the highest volume, we provide a private stub. That means a even more stable infection rate. For more informations see our FAQ.

EASY ADMINISTRATION

Administrative Tasks like viewing the latest infections, setting the ransom price or recrypting your binary can be done with an clean and simple web-interface.

We also have an qualified support, which will help you with any problems. Since this project is still in beta, we are open for any bug-report or feature-request.

PAYMENT SHARE

Your share on the payments you have generated is calculated with the following table. The more volume you generate in one week, the more share on the profit you get.

Example: If you generate a volume of 125 BTC, you get a payout of 106.25 BTC. That are at the moment about 45,000 USD! To get a volume over 100 BTC is not a big deal with the right technique!

Volume/Week	Share
<5 BTC	25%
<25 BTC	50%
<125 BTC	75%
>=125 BTC	85%

THESHADOWBROKERS.BIT

ANNOUNCEMENTS

THESHADOWBROKERS MONTHLY DUMP SERVICE:

JUNE 2017

—BEGIN PGP SIGNED MESSAGE— Hash: SHA1

Welcome to TheShadowBrokers Monthly Dump Service – June 2017

Q: How do I subscribe and get the next theshadowbrokers' dump (June 2017)?

#1 - Between 06/01/2017 and 06/30/2017 send 100 ZEC (Zcash) to this z_address:

zcaWeZ9j4DdBfZXQgHpBkyauHBtYKF7LnZvaYc4p86G7jGnVUq14KSxsnGmUp7Kh1Pgivcew1qZ64iEeG6vobt8wV2siJiq

#2 – Include a “delivery email address” in the “encrypted memo field” when sending Zcash payment

#3 – If #1 and #2 then a confirmation email will be sent to the “delivery email address” provided


Hans Allnutt

Partner

DAC Beachcroft LLP

The logo for DAC beachcroft is displayed within a dark blue rectangular box. The text "DAC" is in a light blue, serif font, while "beachcroft" is in a white, lowercase serif font. A thin light blue horizontal line is positioned at the bottom of the dark blue box.

DAC beachcroft

- Hans Allnutt
- Partner at DAC Beachcroft and leads their Cyber & Data Risk team
- Advises clients on the legal aspects of cyber, data breach and privacy
-  @legallnutt



Legal aspects of cyber and data risk

A variety of legal exposures

Service Interruption

- Contractual breaches
- Regulatory (NIS Dve)

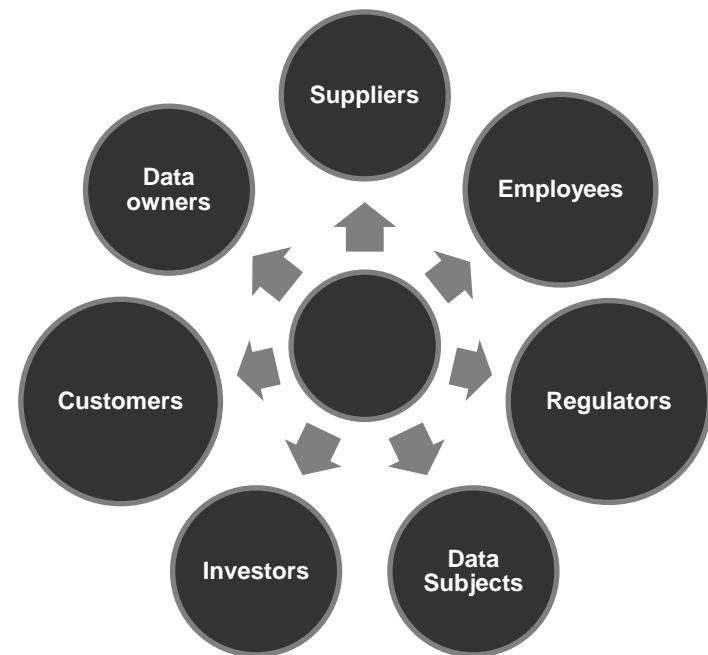
Affected data & information

- Duties of confidentiality
- Regulatory (Data Protection - GDPR, PECR, FCA, PRA)
- Industry Specific (Payment Card, Healthcare)

General Data Protection Reg'n

- 25 May 2018
- Fines 4% Turnover/EUR20m
- Mandatory breach notification

Owed to a variety of stakeholders



GDPR Breach Notification Requirements

Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Notify ICO/DPA

- Unless the personal data breach is **unlikely** to result in a risk to the rights and freedoms of natural persons
- Notification must be made within **72 hours** of the organisation becoming aware of it.

Notify Data Subjects

- All organisations must notify data subjects of breaches that are likely to result in **a high risk** to the rights and freedoms of individuals.
- Notification to individuals must be made **without undue delay**.

Accountability

- Document **any** personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken, to enable supervisory authority to verify compliance.
- Failure to notify can result in a fine of up to EUR10m or 2% of annual global turnover.

Scenario 1

Ransomware



Ransomware

Ransomware is a type of Malware that encrypts or deletes a victims files/sensitive information, with the data not being released until the ransom amount is paid:

- *One third of victims do not get their data back even after paying*
- *40% of businesses in the UK have been hit with Ransomware attacks – with an even higher percentage of individuals being targeted*
- *Criminals netted £1.1BN in ransom payments in the EU in 2016*

Threat Level – **High**

Scenario 1 – Ransomware



The screenshot shows a ransomware payment interface. At the top, there are five service cards: 'FULL RESTORE' for 140\$, 'IMMUNITY' for 30\$, 'REMOVAL' for 30\$, 'FILE RESTORE' for 40\$, and another 'FILE RESTORE' for 2 FREE. Below these is a reference: 'Reference: You full decrypt price is 140 USD.' Underneath is a section for 'Available Payments' showing a Bitcoin icon with the text 'BitCoin accepted here' and a 'Need Help?' button. To the right, there is a 'Public Communication' chat window with a 'Read only' status. The chat contains four messages: 1. 'what kind of email? on what email address?', 2. 'is there a tool included with full restore that decrypts all the files at once?', 3. 'My antivirus has removed the malware. Is the possibility of paying the ransom requested somehow again applicable? Since my antivirus has deleted the ransom-ware program my machine and therefore the link towards the network that could give the decryption key is 99.999% impossible to be restored?', and 4. 'Could you send email to us?'. There is a text input field 'Type your message...' and a 'Send' button.

Am I right, that you paid for 1PC, decrypted it successfully. You tried the same Decryption utility for 2nd PC and it fails?

If yes, as it written above, you should pay for every PC. What the price for second PC? If it is low - we could offer free decryption for your TRUSTED review about first PC.

Waiting for your reply, thank you

This review you need to post on link <http://bit.ly/2ky4Eb2>

Gifted free decode for 798182B07B5530. Please, make a review (with screenshots, payment details, decryption process) on site: <http://bit.ly/2ky4Eb2>

And few others that you will find. Please, make a truthful review as it was. Thank you

7 ok, now i will make some screenshots for proofs. And copy link to site. Thanks.

E Both of my computers have been infected by this. I was able to piece together the price for the first one in bitcoins but my other computer just showed up as being infected too. I will pay the full restore fee, but I dont think I could get the bitcoins in only 3 days, especially starting from scratch.

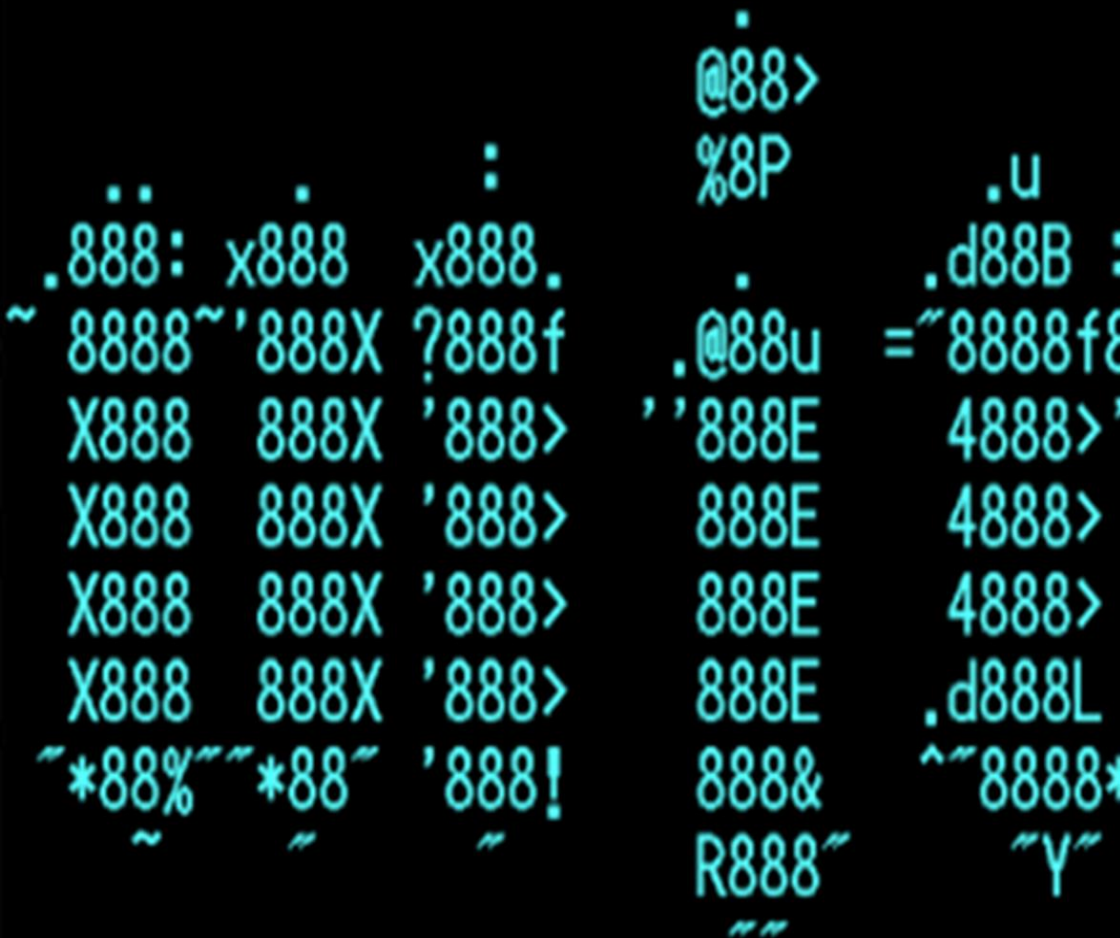
No problem. We disabled deadline for you. Pay asap, please. After this, left a review on <http://bit.ly/2ky4Eb2> and we will send you back some bitcoins

A Thank you admin I got the credit and have purchased! Last user it takes 5-30 minutes depending on your wallet location. my 3 all went in under 15 mins one went in under 5

Please leave a review on site that we have send to you

Scenario 2

Distributed Denial of Service (DDoS) attack



Denial of Service

Distributed Denial of Service (DDoS) is an action that prevents or impairs the authorised use of networks, systems, or applications by exhausting resources, examples include:

- *Using all available network bandwidth by generating unusually large volumes of traffic*
- *Sending illegal requests to an application to cause it to crash*
- *Establishing many simultaneous login sessions to a server so that other users are locked out.*
- *The largest recorded DDoS attack was in 2016 and reached 1.1TBPS*

Threat Level – **Very High**

Scenario 2 – DDoS attack



LIVE TWITTER

Tweets by @GhostSquadHack

Ghost Squad Hackers @GhostSquadHack
optic.tv #Offline GhostSquadHack
@NewWorldHacking

Ghost Squad Hackers Retweeted
@BannedOffline from @GhostSquadHack
attack on optic.tv adding another
spiking as high as 620gbps!!

Ghost Squad Hackers Retweeted
Jacked by SadProphet @FFaroc

- Just before midnight on November 3rd, [REDACTED] received a blackmail e-mail from a cybercriminal group notorious for a recent string of DDoS attacks targeting installations in [REDACTED]
- A DDoS attack quickly followed the threat, lasting 15 minutes.
- Another DDoS attack struck at 11 AM the next morning, at which point [REDACTED] datacenter started mitigation techniques to stop the attack.
- A few hours later at around 2 PM, the attackers targeted their efforts to directly attack the company's ISP and the datacenter. The assault exceeded speeds of a 100Gbps, bringing down hundreds of companies including [REDACTED]
- Left with little choice and mounting pressure from the affected companies and the ISP, [REDACTED] gives in to the ransom demand of 15 bitcoins at 3:30 PM.
- Despite the payment, the attacks continued to such an extent that it disrupted operations across the ISP's entire network.

DDoS ATTACKS

750 Gbps Time: Whole Day

0:30
Minutes Seconds

New World Hackers + Ghost Squad Hackers #2016

0010201

Scenario 3

Data / Intellectual Property Theft



IP/Data Theft

With the accessibility to hacking tools and a burgeoning underground market place, it is no wonder theft of IP/PII Data is on the rise:

- *Cyber Criminal and State level threat actors are the most likely perpetrators data theft.*
- *80% of companies surveyed in Europe are worried about insider threats*
- *Malware and weak passwords are the most common attack vectors*
- *Most common data stolen:*
 - *Credit Cards*
 - *Customer Data*
 - *Intellectual Property*

Threat Level – **Very High**



Scenario 3 – Data / Intellectual Property Theft



Dear all @ XXXXX: And whom this may concern

You might want to pass this message on to the right person quickly.

We are thedarkoverlord (we've recently hacked Netflix, Disney, many healthcare companies, banks etc.), and found your security to be lacking. We were able to compromise your systems over the last few days and have managed to extract over 500,000 customer records from your sites.

We were also able to compromise your Gmail data and have lots of sensitive internal emails and HR conversations- which trust us makes for GREAT reading!

This is no joke! Here is a sample so you can validate our claims <http://pastebin.com/LUMVMS>

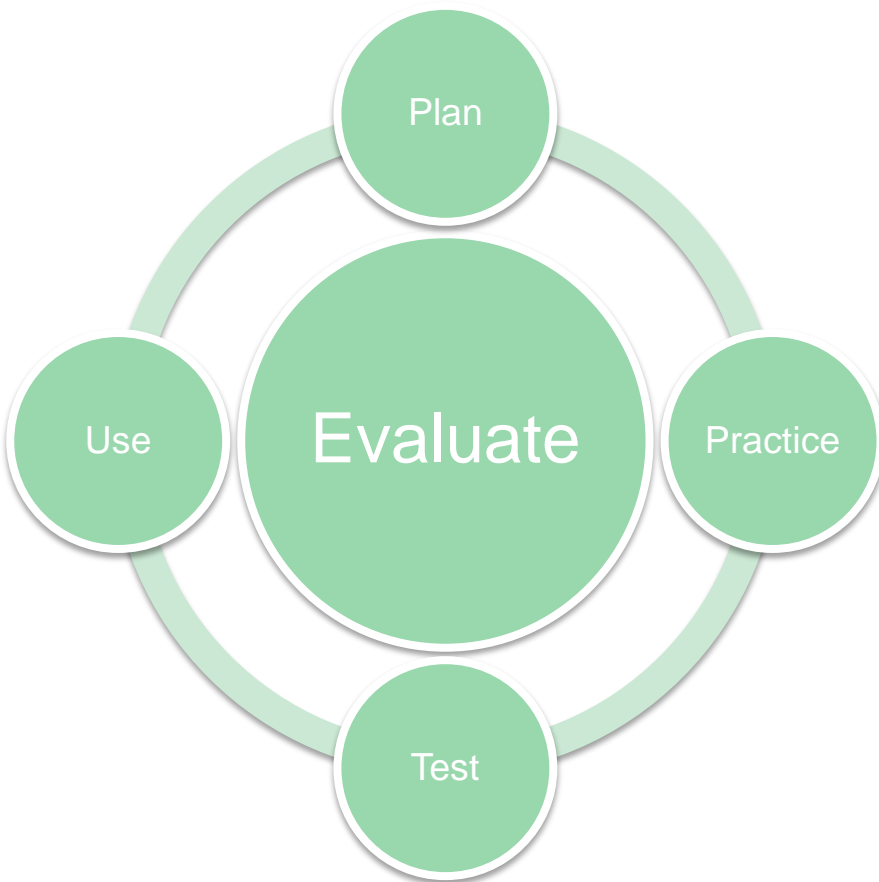
We will start to leak this information to the press over the next few hours. If you do not pay us **150 Bitcoins** to this Wallet **1QAc9S5EmycqjzzWDclyiWzr9jJLC8sLiY** - then we will publicly name and shame you to the press.

If you do not pay us in the next few hours the price will go up by **10 Bitcoins per hour!!** We will also be selling your customer data on all the darknet market places at the end of the day. This will get considerably worse for you if you don't pay us.

As always, we are open to communication and discussion with all of our valued business partners, but if you contact the police then we will immediately leak the data.

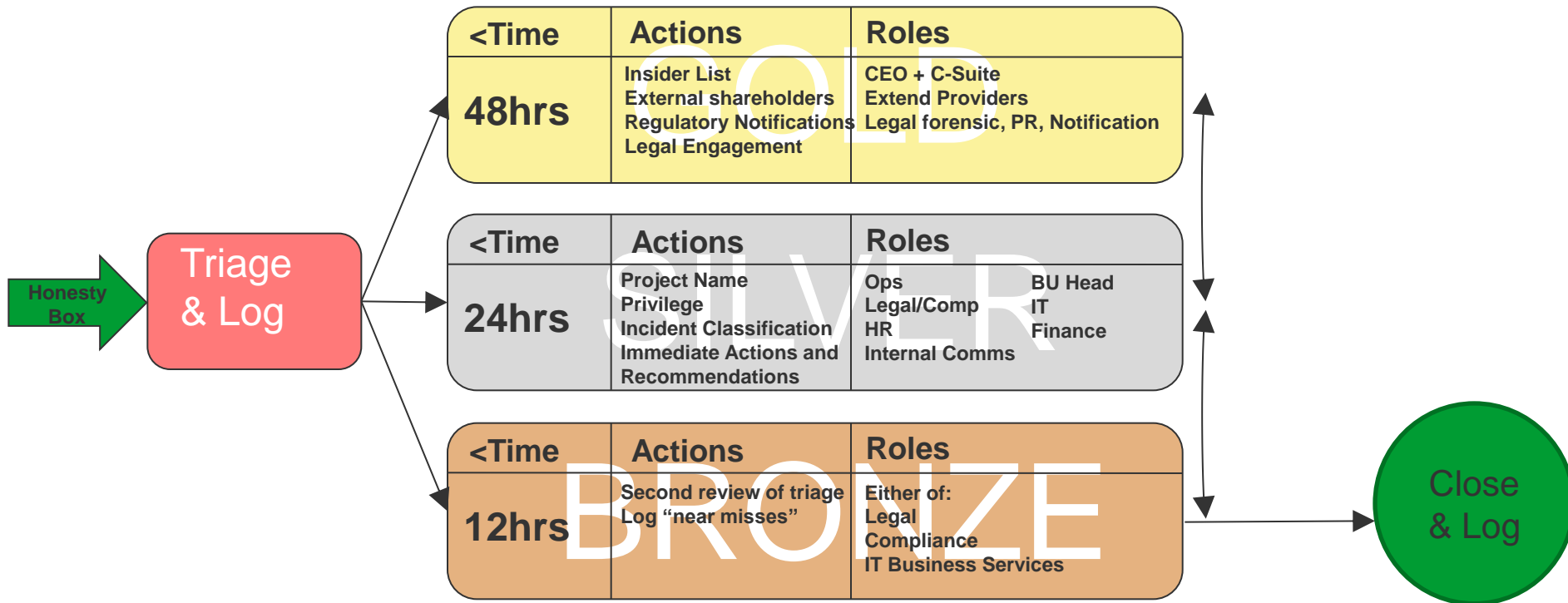
Until next time,
thedarkoverlord
Professional Adversary
World Wide Web, LLC

Data Breach Planning



- Who needs to know (roles)?
- Who does not need to know (does the CEO need to know everything)?
- What are the escalation triggers?
- How will you communicate (email, phone, alternative)?
- Who is responsible for making decisions and do they have authority?
- How will they make decisions – what information do they need?
- When does this all need to be done by?

Internal Data Breach Plan



Final Thoughts

“One of the things I say to people is that [when you’re] employing 70,000 people worldwide, providing public services, there is one thing that I can guarantee you:

24 hours a day, 365 days a year, someone somewhere is doing something really stupid.”

Nicholas Soames OBE, Serco plc