

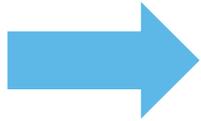


# AIRMIC LIVE

Responding to and costing a ransomware attack

25 November 2020

**SubSure<sup>™</sup>**



# SubSure

Manufacturer for submarine parts

## What's happened?

- Hackers have accessed the IT infrastructure and detonated ransomware
- All internal and external systems are down
- All screens display a ransom note



**\*\*\*GREETINGS!\*\*\***

**CrazySnakes have left you a  
present AMIGOS**

**Pay 20 bitcoin to release your  
data**

**Bitcoin wallet:t38b1mmi93hs71bs0h2**



**Insurers' 24/7 hotline**

# Legal

What is the legal team going to do for us?

- Investigate - What's happened?
- Notify ICO and Action Fraud
- Coordinate other vendors
- Advise on third party notification and general strategy
- Advise on exposures

**// Do we go to our existing  
IT suppliers or a specialist  
forensics firm?**

# IT Forensics

What is the forensic team going to do for us?

- Close down vulnerability
- Assist with data restoration from backups
- Analyse scope and root cause of breach
- Look for evidence of exfiltration

**// Do we communicate  
with the threat  
actors?**

# PR Consultants

What is the PR Team going to do for us?

- Manage media response (pro-active -V- reactive)
- Develop key messaging for customers and employees
- Assess stakeholder matrix
- Prepare press releases and social media announcements

**// What do we say to  
customers and staff?**

# Immediate messaging

What are we saying to customers and employees?

- *“Experiencing some IT issues”*
- *“Working hard to restore functionality”*
- Reassuring messaging to key defence customers
- Employees - reassuring message and promise of updates

# Two days in...

- Restoration going well - 60% of systems back online
- No wider media coverage
- **BUT...**



10:19



Neil B

Hey there! I am using WhatsAp...



23 November, 00:00

Ollie/Tom, need to speak URGENTLY  
10:16

It looks like there's been significant  
exfiltration on this one  
10:17

We're looking into it, but seems there  
may have been around 100gb exfiltrated  
10:18

Call me ASAP  
10:19



12:40 80%

**Tweet**

 **CrazySnakes\$**   
@CrazySnakes

**!Hacked! SUBSURE -**  
[www.subsure.com](http://www.subsure.com)  
**\*\*\*We got the lot. Here's 5gb for FREE!!! -** <https://mega.nz/hins682gy5fyj53>

12:39 • 02/10/2020

**DRAFT**

**1042-S** Foreign Person's U.S. Source Income Subject to Withholding **2019**

**01 5000.00** **14** **250** **32**

**TIGER CO**

**OC**

**884 TIGER WAY**

**CHEYENNE WY 82001**

**LION INC** **SZ**

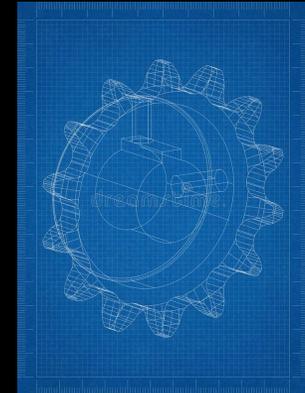


**TERMS AND CONDITIONS OF EMPLOYMENT**

Employee: [Name of Employee] (The "Company")  
Employer: [Name of Employer]

In accordance with the requirements of Section 1 of the Employment Rights Act 1996, it is acknowledged that employment given under certain particular of the terms and conditions applicable to your employment by the Company:

- 1. START DATE:**  
Your employment with the Company will commence on [Date] [Month] [Year] and your period of continuous employment with the Company shall be calculated from that date.
- 2. PROBATIONARY PERIOD:**  
Your employment with the Company commenced on [Date] [Month] [Year] and your period of continuous employment with the Company for probationary purposes commenced on [Date].
- 3. PROBATIONARY PERIOD:**  
You will have a probationary period of 1 (one) [Month] [Year]. During your probationary period your performance will be reviewed by your line manager. Your probationary period will be extended at the discretion of the Company. During your probationary period either party may terminate your employment by giving one week notice in writing.
- 4. LOCATION:**  
Your normal place of work is [Address] [Postcode] [City] [County] [Country].
- 5. JOB TITLE AND DUTIES:**  
Your job title is [Job Title]. Please refer to your role profile for the main duties and responsibilities associated with this role. In addition to the duties which the job normally involves, you agree to perform any other duties which may be assigned to you.



Outlook interface showing an email from FIVE John Smith.

**From:** FIVE John Smith  
**To:** [Name]  
**Subject:** [Subject]

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

**LIVE**

breakyourrowanews.com

**BREAKING NEWS**

# **MAJOR DEFENCE DATA LEAK**

**14:38**

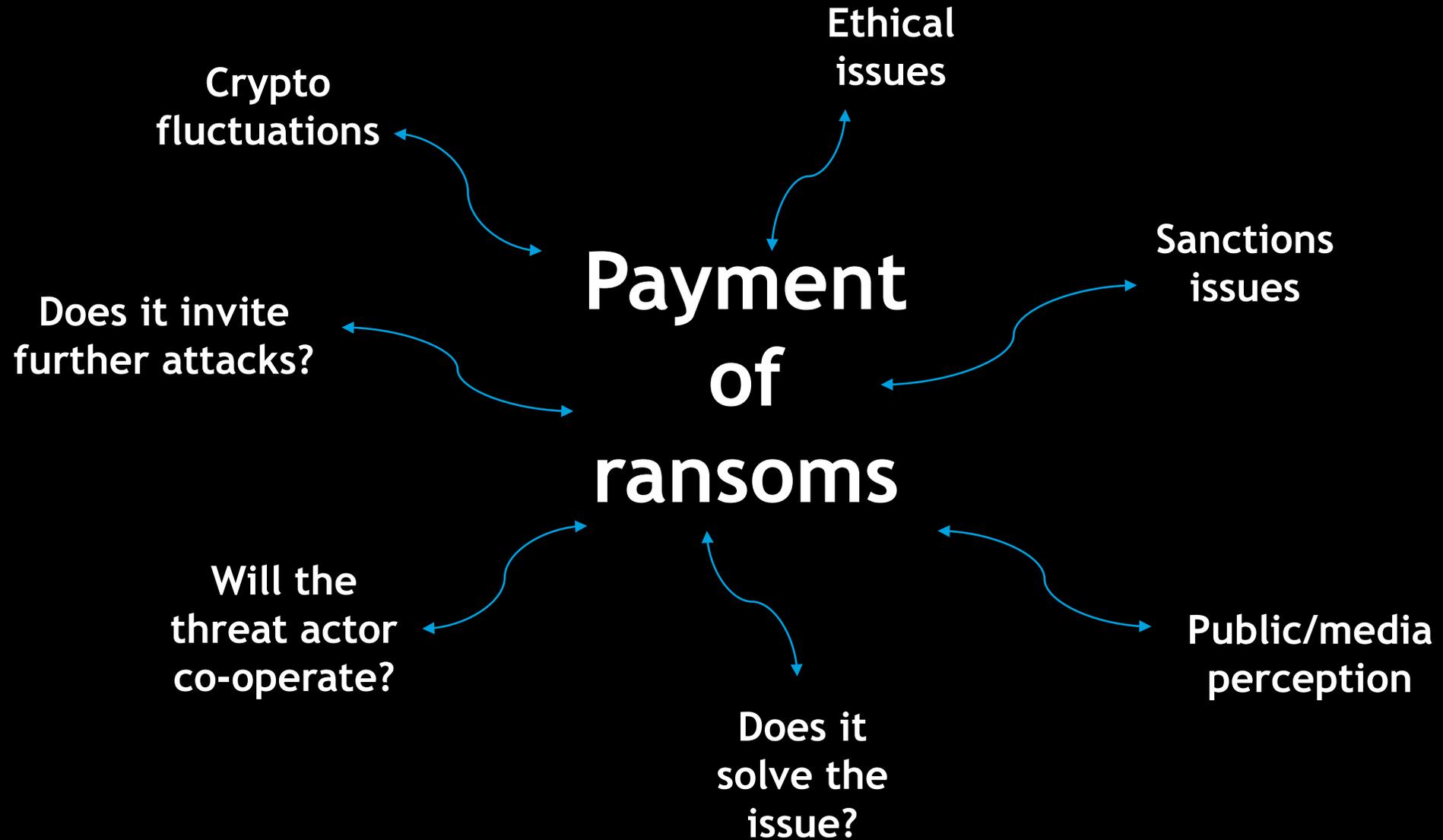
**THOUSANDS OF SUBSURE DOCUMENTS RELEASED BY ATTACKERS**

**// What do we say to the media, customers and staff?**

## Key Messaging

- Confirm attack and data loss
- Focus on the fact it's a criminal act
- We are investigating with a team of experts and engaging with the Police and regulators
- We will be communicating with any affected individuals and customers
- Cannot comment further at this time
- Follow up with an immediate message to customers and staff

// Should we pay  
the ransom?



// How much is this going to cost us?

SubSure CEO

# Potential exposures

- Fees of response team - £200,000+
- Ransom payment - 20 BTC = £280,000
- Third party/customer/employee claims -
- Business interruption and lost contracts
- Regulator fines
- Hidden notification costs



£1m+

# Key Contacts



**Tom Pelham**

Partner

Kennedys

07818 573 330

Tom.Pelham@kennedyslaw.com



**Ollie Dent**

Partner

Kennedys

07584 391 370

Ollie.Dent@kennedyslaw.com



Want to know more?

