whitleypenn

CYBERSECURITY RISK IN THE ENERGY SECTOR

JOHN WILLIAMSON, CPA.CITP, CIA, CFE, CISA

HLB WE ARE AN INDEPENDENT MEMBER OF THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

1

JOHN WILLIAMSON

whitleypenn

Risk Advisory Services Partner

- 12 years of experience in public accounting
- Internal Audit, IT Audit, SOX 404, SOC Reporting, and Cybersecurity services
- Board of Governors, IIA Dallas Chapter
- IIA Manager Roundtable, Steering Committee
- Father of **five (5)** children
- **Failed musician**
- Bachelor of Music from Southern Methodist University
- Master of Music from Rice University
- Master of Accounting from University of Texas at Dallas

HLB WE ARE AN INDEPENDENT MEMBER OF THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

2

2

KEY DEFINITIONS

whitleypenn

Incidents vs. Breaches

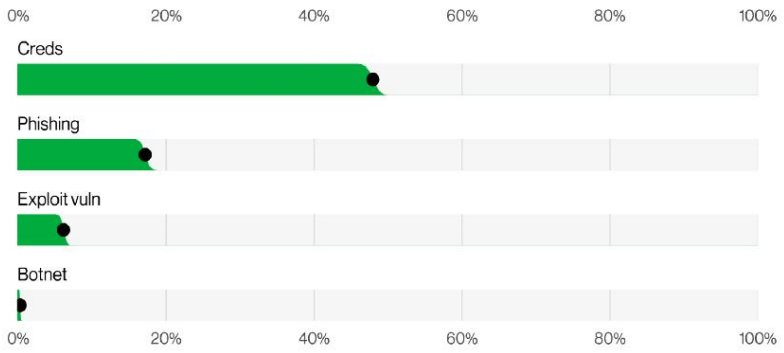
- An **incident** is a security event that compromises the integrity, confidentiality, or availability of an information asset.
- A **breach** is an incident that results in the confirmed disclosure – not just potential exposure – of data to an unauthorized party.

Data at Risk

- **Personal data** are data that allow the identification of a person directly or indirectly: Name, address, telephone number, SSN, DOB, Health Information, Cookie ID, etc.
- **Payment data** are data that will allow an individual or organization to process transactions on one's behalf: Credit card number, card expiration date, CV number, bank account number, etc.
- **Proprietary data** are data that is owned by an individual or organization that is involves trade secrets or is privileged.
- **Credentials** are data that allow an individual to authenticate, or prove, that they have the right to access information: Username and password, passcodes, etc.

3

3



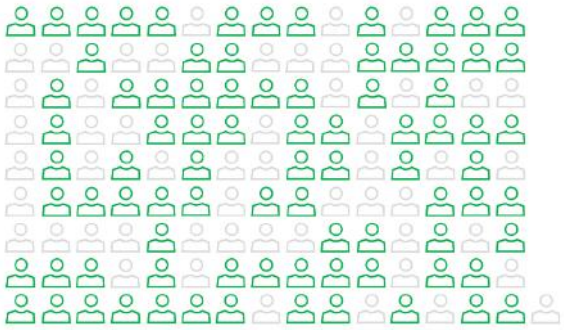
TRENDS IN DATA BREACHES

There are four key paths leading to your assets: Credentials, Phishing, Exploiting Vulnerabilities, and Botnets. These four pervade all areas of recently reported breaches, and no organization is safe without a plan to handle them all.

Source: Verizon Data Breach Investigation Report

4

4



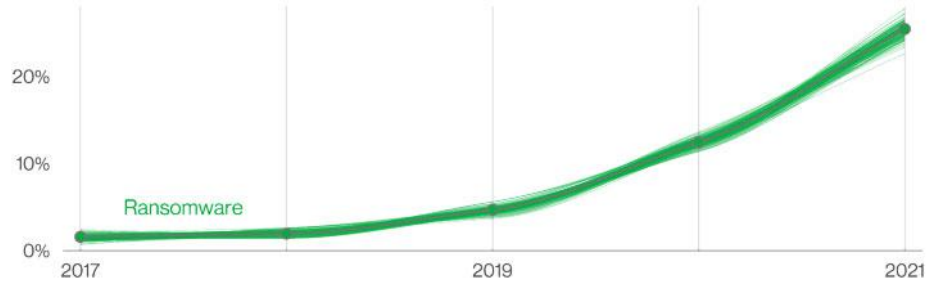
TRENDS IN DATA BREACHES

This past year illustrated how one key supply chain breach can lead to wide ranging consequences. Supply chain was responsible for 62% of System Intrusion incidents this year.

Source: Verizon Data Breach Investigation Report

5

5



TRENDS IN DATA BREACHES

This past year, ransomware has continued an upward trend with an almost 13% increased use in compromises, for a total of 25%.

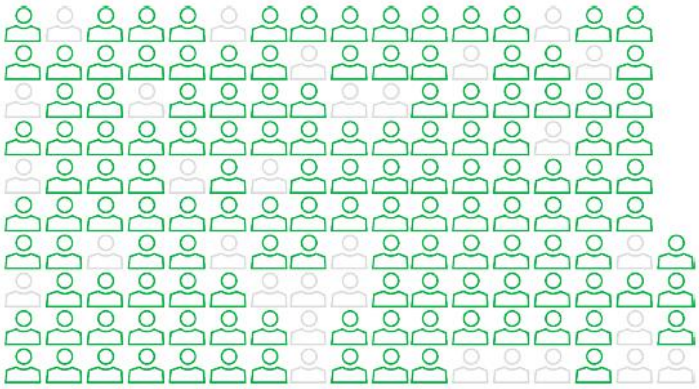
Source: Verizon Data Breach Investigation Report

6

6

TRENDS IN DATA BREACHES

The human element continues to drive breaches. This year 82% of breaches involved the human element. Whether it is the Use of stolen credentials, Phishing, Misuse, or simply an Error, people continue to play a very large role in incidents and breaches alike.



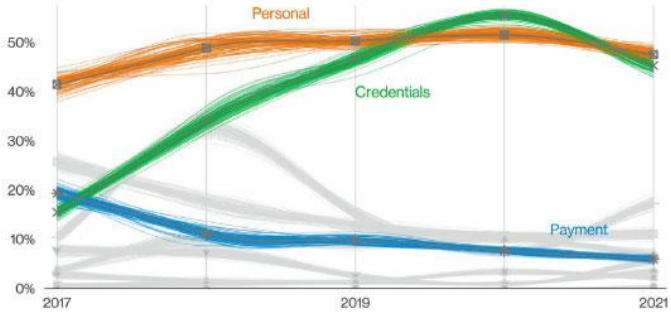
Source: Verizon Data Breach Investigation Report

7

7

TRENDS IN DATA BREACHES

Payment data is on the decline. The top two data types under attack are credentials and personal data, since they can be reused in other attacks.



Source: Verizon Data Breach Investigation Report

8

8

ENERGY SECTOR TRENDS

96% external threat actors
4% internal threat actors

Actor motives: 78% Financial and 22% Espionage

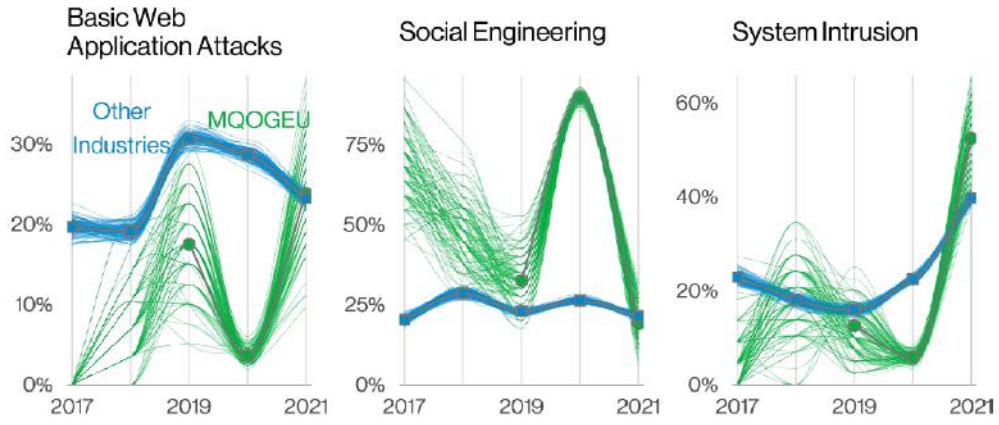
Credentials and Personal Data are the most sought-after data

Source: Verizon Data Breach Investigation Report

9

9

ENERGY SECTOR TRENDS



Source: Verizon Data Breach Investigation Report

10

10

CYBERSECURITY POP QUIZ

whitleypenn

What is the most common attack vector used by cybercriminals in a ransomware attack?

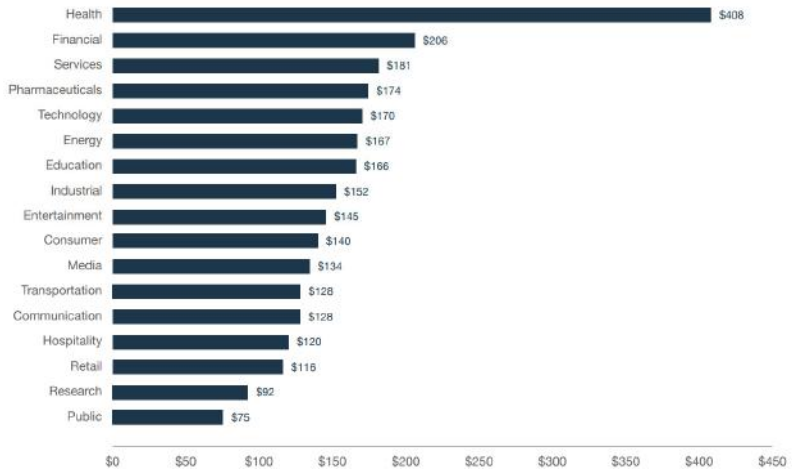
A. Use of stolen credentials
B. Phishing
C. Exploiting misconfigurations/vulnerabilities to install malware
D. Stealing servers and leaving a ransom note

Source: Verizon Data Breach Investigation Report

11

CYBERCRIME FINANCIAL IMPACT *(COST PER RECORD, BY INDUSTRY)*

whitleypenn



Source: Ponemon Institute Cost of a Breach Report

12

CYBERCRIME FINANCIAL IMPACT

whitleypenn

13th largest global economy

The mirror image of contemporary capitalism

$2 million annual salary for highest earners

20% of profits reinvested (~ $300 billion)

Source: Federal Bureau of Investigation

CYBERCRIME FINANCIAL IMPACT

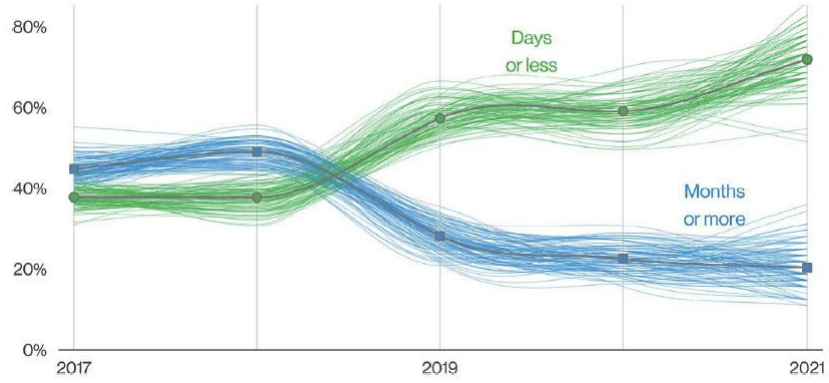
whitleypenn

Costs of Cybercrime	1.5 Trillion USD (2021)
	1% of global GDP
	$8.9M average cost of US breach

Source: Federal Bureau of Investigation

TRENDS IN DATA BREACHES

whitleypenn



Amount of time to detect a breach from the point of compromise.

HLB WE ARE AN INDEPENDENT MEMBER OF THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

Source: Verizon Data Breach Investigation Report

15

15

whitleypenn

CYBERSECURITY POP QUIZ

Which of the following combinations DOES NOT qualify as multi-factor authentication (MFA).

A. Username/password and thumbprint.
B. Facial recognition and SMS authentication code.
C. Username/password and selecting 3 pictures that include a school bus.
D. Key fob and knowledge of a keypad pass code.

HLB WE ARE AN INDEPENDENT MEMBER OF THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

16

16

CASE STUDY 1: SHELL BREACH

In March 2021, Shell plc issued a press release indicating that it was the victim of a ransomware attack.

During a forensic investigation, security experts traced the breach to a specific piece of hardware, a File Transfer Appliance (FTA) produced by Accellion.

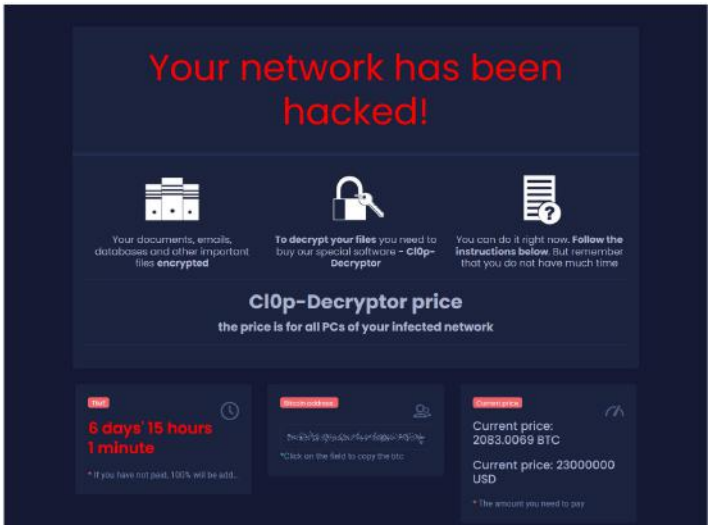
17

17

CASE STUDY 1: SHELL BREACH

Accellion engaged FireEye, a security forensics firm, to perform an analysis. They attributed the attack to UNC2546, which has ties to the CLoP ransomware gang and FIN11, an organized crime group.

Evidence suggests that the CLoP ransomware gang operates out of Ukraine and other eastern European countries.



18

18

CASE STUDY 1: SHELL BREACH

- By revenue, Shell is the second-largest investor-owned oil company in the world and the largest company headquartered in the United Kingdom. It is the 8th largest company in the world.
- In December of 2020, hackers targeted Accellion's File Transfer Appliance (FTA), which had previously-reported known vulnerabilities.
- Accellion's FTA was more than 20 years old and was at "end-of-life." The FTA used CentosOS6, a Linux-based operating system that was no longer supported as of November 2020.
- The attackers targeted the vulnerable system through a SQL injection, which injects malicious code into an application through a vulnerability.
- The attacker then leveraged a malicious script to steal data from the FTA.

19

CASE STUDY 1: SHELL BREACH

SHELL RECEIVED A BARRAGE OF EXTORTION EMAILS:

Hello!

Your network has been hacked, a lot of valuable data stolen. <description of stolen data, including the total size of the compressed files> We are the CLOP ransomware team, you can google news and articles about us. We have a website where we publish news and stolen files from companies that have refused to cooperate. Here is his address http://[redacted].onion/ - use TOR browser or http://[redacted].onion.dog/ - mirror. We are visited by 20-30 thousand journalists, IT experts, hackers and competitors every day. We suggest that you contact us via chat within 24 hours to discuss the current situation. <victim-specific negotiation URL> - use TOR browser We don't want to hurt, our goal is money. We are also ready to provide any evidence of the presence of files with us.

This is the last warning!

If you don't get in touch today, tomorrow we will create a page with screenshots of your files (like the others on our site), send messages to all the emails that we received from your files. Due to the fact that journalists and hackers visit our site, calls and questions will immediately begin, online publications will begin to publish information about the leak, you will be asked to comment.

20

CASE STUDY 1: SHELL BREACH

On March 16, 2021, Shell issued the following press release:

The ongoing investigation has shown that an unauthorized party gained access to various files during a limited window of time. Some contained personal data and others included data from Shell companies and some of their stakeholders. Shell is in contact with the impacted individuals and stakeholders and we are working with them to address possible risks. We have also been in contact with relevant regulators and authorities and will continue to do so as the investigation continues.

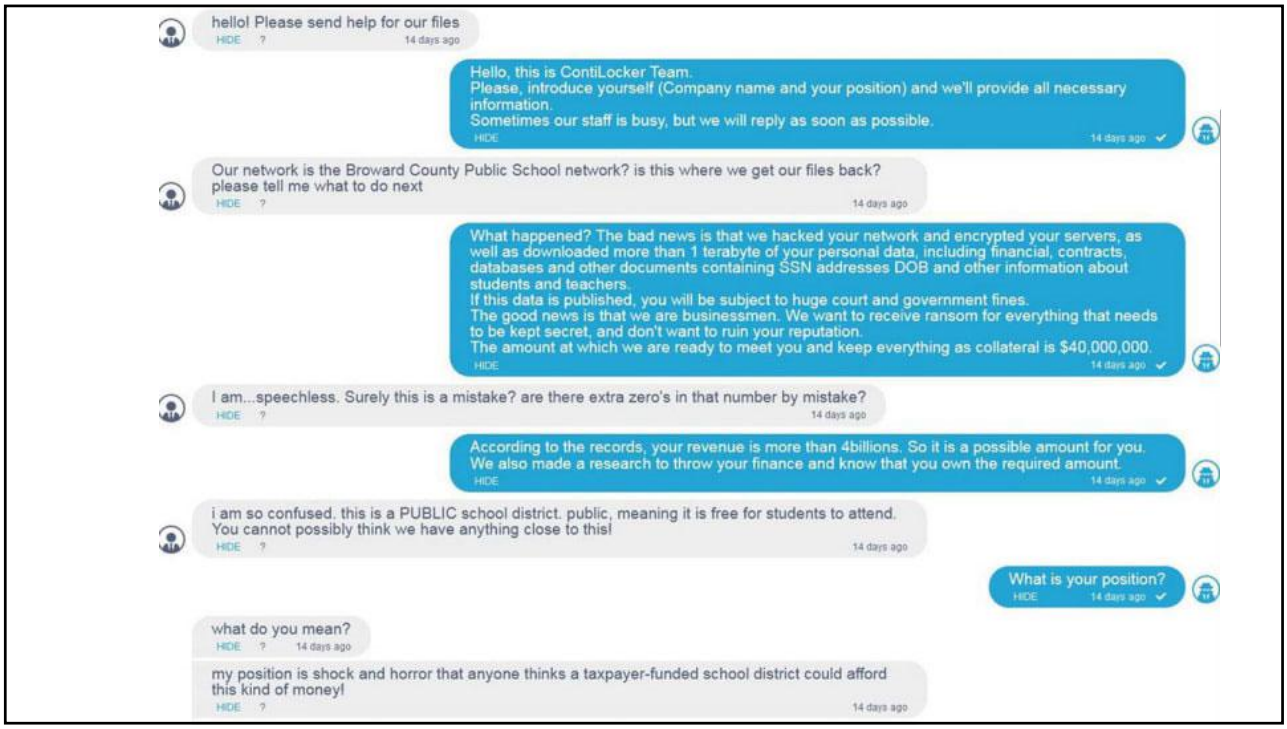
Shell has not disclosed whether it paid the ransom.

CASE STUDY 1: SHELL BREACH

Other Companies Impacted by the Accellion Vulnerability:

- Bombardier, Inc.
- Jones Day
- The State of Washington
- Qualys, Inc.

Open-source detection tools have been released to the public and the end-of-life FTA has been retired.

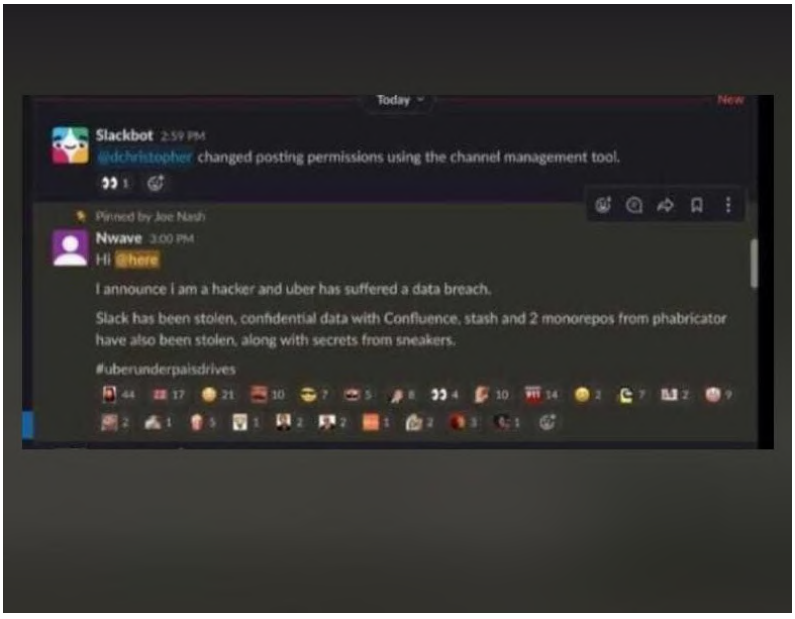


23

CASE STUDY 2: UBER

On September 16, 2022, the ride-hailing company, Uber, first discovered that it was breached after a message posted to the Company-wide slack channel.

The attack is attributed to an 18-year-old who claims to have tricked an employee into providing their credentials by posing as an employee in IT.



24

24

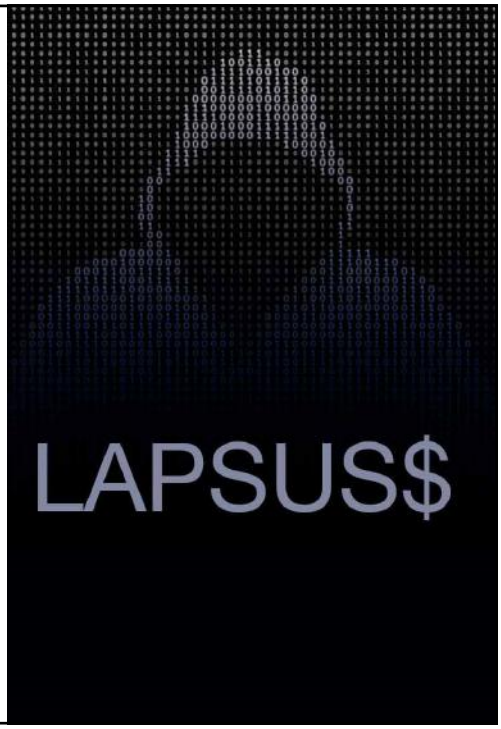
CASE STUDY 2: UBER

On Monday of this week, Uber disclosed that the attack was conducted by a member of LAPSUS$ who goes by the moniker Tea Pot. The hacker also has taken credit for a recent breach at Rockstar Games over the weekend.

Uber states that a contractor had their personal device compromised with malware and their corporate account credentials were stolen and sold on the dark web.

The attacker repeatedly tried logging on with the contractor's credentials, each time the contractor received an MFA request to approve on his mobile device. The contract eventually accepted on, leading to the compromise

25



25

CASE STUDY 2: UBER

whitleypenn

- Once the corporate account was compromised, the attacker accessed several other employee accounts which ultimately gave the attacker elevated permissions to a number of tools, including Google Workspace and Slack.
- The threat actor posted a message on a companywide Slack channel and reconfigured Uber's OpenDNS to "display a graphic image to employees on some internal sites," the Company said.
- The Company took swift action to disable internal tools, resent access permissions for administrator accounts, and lock down the Company's code database. Uber is currently cooperating with the FBI and DOJ.

HLB WE ARE AN INDEPENDENT MEMBER OF THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

26

26

CASE STUDY 2: UBER

- LAPSUS$ is an international hacker group known for cyber attacks against tech companies, with member typically ranging between the ages of 16 and 21.
- The group's assumed *MO* is obtaining access to a victim organization's corporate network by acquiring credentials from privileged employees. These credentials were acquired in a number of ways, including recruitment or hacking privileged employees. Lapsus$ then uses remote desktop or network access to obtain sensitive data, such as customer account details or source code.
- Notable hacks in 2022: Microsoft, Mercado Libre, Samsung, Okta, T-Mobile, Cisco, and Rockstar Games.

27

27

CASE STUDY 3: OIL & GAS EMAIL COMPROMISE

Local upstream oil and gas company email compromise for $250,000

- What happened:
  - Accounting Manager gets an email from the COO asking to transfer funds to a new vendor.
  - The email included correspondence between the COO and the new vendor discussing the initial payment and a change in payment instructions.
  - Emails from the vendor claimed that the original bank account had been closed, which included a forged account closing letter.
  - The Accounting Manager released the funds, with approval from the Controller.
  - Three weeks later, the vendor inquired about the payment claiming it was never received.

28

28

CASE STUDY 3: WHAT WENT WRONG

- Multi-factor authentication (MFA) was rolled out one year prior, but it was made optional to employees.
- The COO never enabled MFA and the email account was hacked by using a remote access terminal.
- The bad actor setup a rule to automatically delete any emails sent from the attacker.
- After one to two weeks of monitoring the COO's emails, the attacker created a scheme using intelligence from email monitoring.
- There was a lack of call back procedures for payment instruction changes.

29

29

CYBERSECURITY POP QUIZ

Ransomware victims that pay the ransom receive the decryption key more than 50% of the time.

A. True

B. False

30

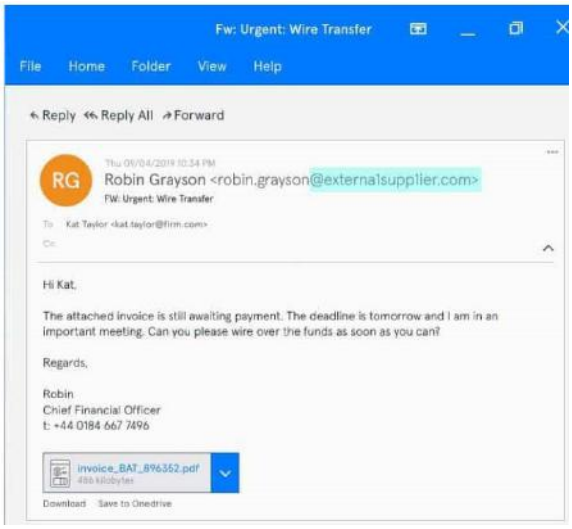
30

ELECTRONIC VENDOR FRAUD ATTACK METHODS

whitleypenn

Domain Impersonation

Domain impersonation occurs when an attacker appears to use a company's domain to impersonate a company or one of its employees. This can be done by sending emails with false domain names which appear legitimate, or by setting up websites with slightly altered characters that read as correct.



31

ELECTRONIC VENDOR FRAUD ATTACK METHODS

whitleypenn

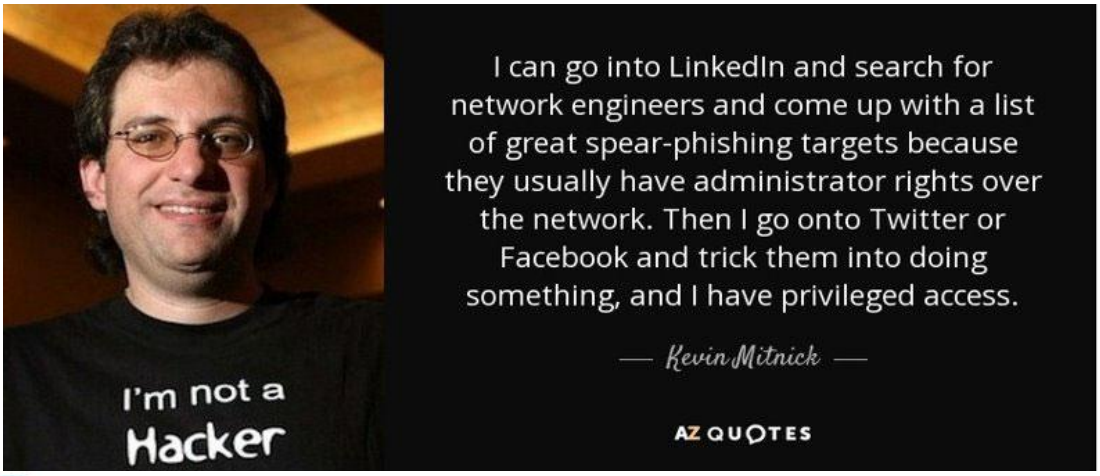
Spoofing

The attacker modifies the sender's email address to identically match a trusted source.

```
Return-Path: <m.mouse@disney.com>
X-Original-To: robertbateman@email.com
Delivered-To: robertbateman@email.com
Received: from localhost (cybercrime .org [91.99.504.210]) (using TLSv1.2 with cipher
 ECDHE-RSA-AES256-GCM-SH4562 (256/256 bits)) (No client certificate requested) by
 mailin005.disney.com (Postfix) with ESMTPS id 9B910401007A for
 <robertbateman@email.com>; Wed, 13 Jan 2021 15:38:36 +0000 (UTC)
Received: by localhost (Postfix, from userid 33) id 3F138221CB; Wed, 13 Jan 2021 10:38:36
 -0500 (EST)
Authentication-Results: mailin005.disney.ch; dmarc=none (p=none dis=none)
 header.from=disney.com
Authentication-Results: mailin005.disney.ch; spf=none smtp.mailfrom=m.mouse@disney.com
Authentication-Results: mailin005.disney.ch; dkim=none
To: robertbateman@email.com
Subject: Hi There
From: "Mickey Mouse" <m.mouse@disney.com>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: m.mouse@disney.com
Reply-To: m.mouse@disney.com
Content-Type: text/plain
Message-Id: <20210113153836.3F138221CB@localhost>
```

This is an example of an email header. You can see who the genuine sender is, who they're pretending to be, and that DMARC, SPF, and DKIM aren't enabled.

32



33

33

CYBERSECURITY BEST PRACTICES: "TOP 10"

1. Cybersecurity Governance
2. Data Classification and Mapping (Bridging the IT/OT gap)
3. Third-Party Risk Management
4. Security Awareness Training
5. Incident Response Planning
6. Asset Inventory
7. Vulnerability Management
8. Restriction of privileged access
9. Perimeter defenses and anti-malware
10. Recoverability

34

34

VENDOR MAINTENANCE BEST PRACTICES

- Email sandboxing for all inbound emails & MFA.
- Corroborate all request for changes to vendor address and/or banking information by phone, NOT email. Use previously known numbers you know are correct and not the numbers provided in an email or text request.
- Revise forms to require vendors to provide BOTH old and new bank routing and account numbers or billing addresses when requesting a bank change or a payment mailing change.
- Remove vendor change forms from website. Have vendors contact staff directly for forms.
- Consider two-party sign-off on payment instructions.
- Require documentation (specific forms/voided checks/bank letters).
- Conduct end user training.
- Incident response planning.

35

Contact Information:

John Williamson
214.393.9398
John.Williamson@whitleypenn.com

36

36