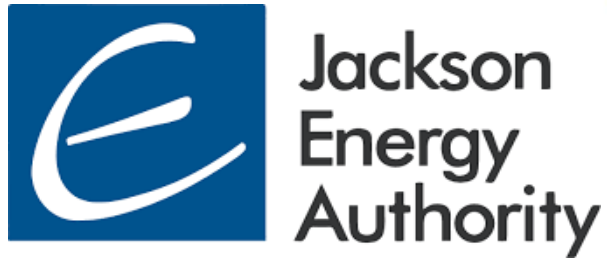


# Incident Response Plan

*Are you ready?*



# Incident Response back in the days... true story







Jackson  
Energy  
Authority

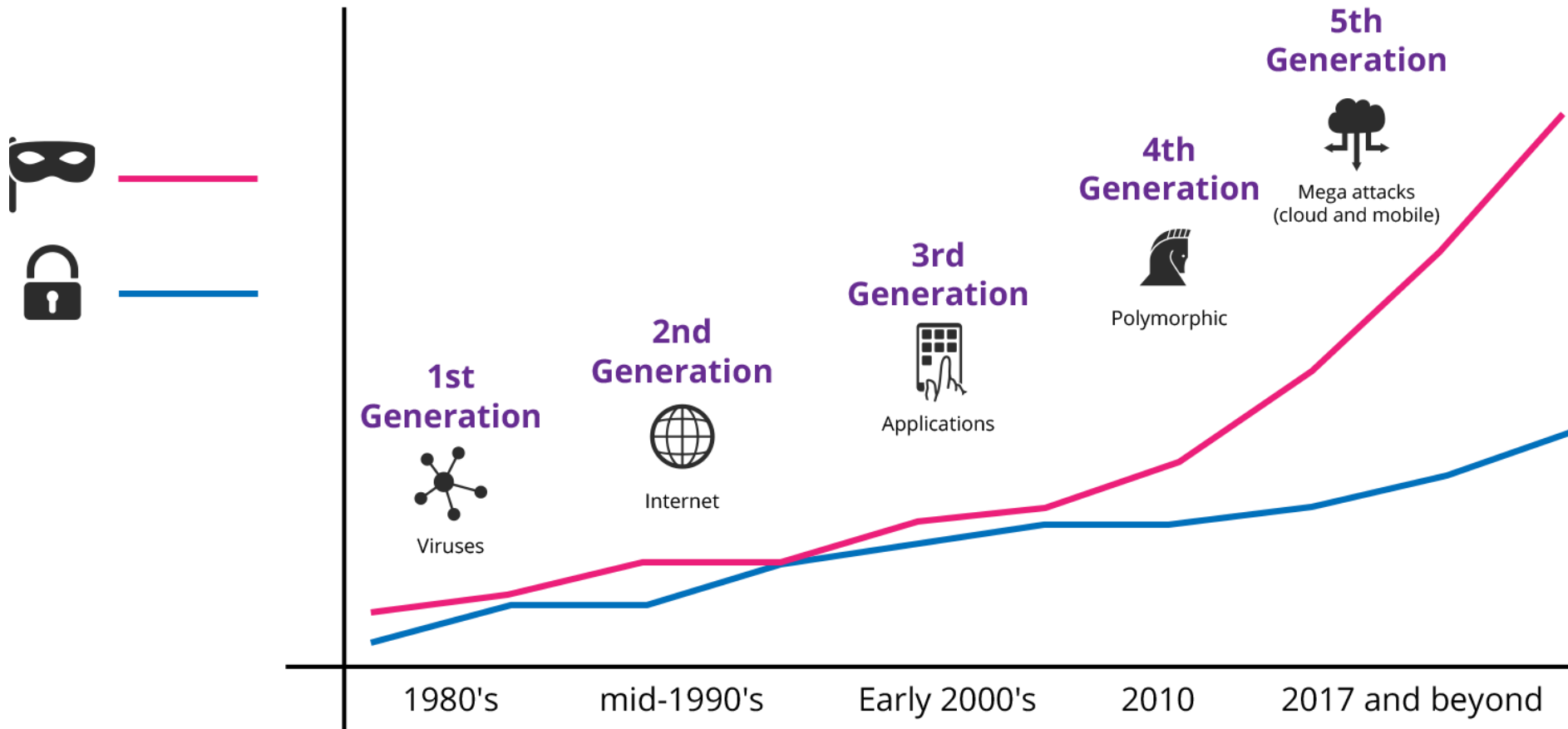
## Joey Perry, CISM, CDPSE

IT Operations Manager

[jperry@jaxenergy.com](mailto:jperry@jaxenergy.com)



# The good guys are way behind and the gap is exponentially growing





# What does a cyber incident look like?





# What does a cyber incident look like?



# Why is it so hard ?

- Unknown area, fear of the unknown
- Intimidating figures
- Loss of control
- Multiple stakeholders
- Real management pressure
- Public interest
- No planning at all





# Consequences

- Mistakes
- Disorder & chaos
- Acceleration & amplification of the situation losses





**So where do we start ?**





***“Know your enemy and know yourself and you can fight a hundred battles without disaster”***

**(Sun Tzu)**

- Who are your threat actors
- What are they after
- Your capabilities
- Your environment
- Your tools
- Who should be part of an IR process



# Ransomware as a Service

The screenshot shows the 'Making a dropper' page on the Satan RaaS website. The page includes instructions for creating a dropper and provides code snippets for PowerShell and Python. The PowerShell code uses the System.IO.File class to read and write files. The Python code uses the sys, getopt, ntpath, and os modules to perform XOR encryption. Below the code, there are usage instructions for both languages. At the bottom, there is a 'Generate' section with input fields for URL, Key, and a Captcha image.

### Making a dropper

1. Use one of the xor functions below to encrypt your ransomware.
2. Upload the encrypted ransomware to your web server.
3. In the form below, enter the url to the file, the key you used to encrypt and click on "Generate".
4. Follow the usage instructions

### Xor

#### Powershell

```
param ([Parameter(Mandatory=$true)][string]$source, [Parameter(Mandatory=$true)][string]$output, [Parameter(Mandatory=$true)][string]$key)
$contents=[System.IO.File]::ReadAllBytes($source)
for ($i=0;$i -lt $contents.count; $i++){
    for ($j=0;$j -lt $key.length;$j++){
        $contents[$i] = $contents[$i]
    };
}
[System.IO.File]::WriteAllBytes($output, $cont
```

#### Python

```
#!/usr/bin/python
import sys, getopt, ntpath, os
def xor(source, output, key):
    contents = bytearray(open(source, "rb")
    for i in range(len(contents)):
        for j in range(len(key)):
            contents[i] ^= ord(key[
    with open(output, 'wb') as output:
        output.write(contents)
```

#### Usage

```
powershell -ExecutionPolicy Bypass -File script
python script.py -s "source.exe" -o "output.exe"
```

### Generate

URL:

Key:

Captcha:

The screenshot shows the account dashboard and the 'Create a malware' form on the Satan RaaS website. The dashboard includes statistics for Malwares, Infections, and Paid, along with a Bitcoin balance and a 'Withdraw' button. The 'Create a malware' form has fields for Ransom, Multiplier, Note, Proxy, and Captcha, and a 'Create new' button. A blue arrow points to a warning box at the bottom of the form.

### Account Dashboard

Malwares	0
Infections	0
Paid	0

Balance: 0.00000000 B

Your bitcoin address:  [Withdraw](#)

### Create a malware

Ransom:  Ransom in BTC (min 0.1)  
Use "." as decimal separator.

Multiplier:  Optional  
Used to multiply the ransom by X times after Y days.

Multiplier (Days):  Optional  
Days before the ransom multiplier.

Note:  Optional  
Notes are private, and used only to keep track of your victims.

Proxy:  Optional  
Read about how to set up a gateway proxy [here](#).

Captcha:

[Create new](#)

Do not upload your malware to VirusTotal and/or any other online scanner.

# Ransomware as a Service

Satan

Malwares Droppers Translate Account Notices Messages Logout

## Translation guidelines

1. All fields must be filled.
2. Anything between "%" should be only copied and not translated.
3. The field "English" should be filled with the name of the language you're translating (e.g Deutsch, Español).
4. The characters used must be UTF-8 supported.
5. Only one translation is allowed per day.

The translations are manually checked and added once a day. Duplicates are ignored.

Languages already translated to:

English / Português / עברית / Deutsch / Italiano / Español / Русский / Latviski

English

Your personal files have been encrypted. In order to decrypt them you'll have to pay %RANSOM% BTC

If the payment is not made until %LIMIT%, the cost for the private key will increase to %RANSOM\_MULTIPLIED% BTC



# Ransomware as a Service

Plastic • One Month C&C Subscription \$60 USD

- 250kb Unique EXE - Combo Encrypter/Decrypter
- Compatible with Windows XP to Windows 10
- You receive 100% of the ransom paid by the victims
- Supports Delayed Start, Mutex, and Task Manager Disabler
- Ransomware still works if you don't continue your C&C subscription
- Free support with active C&C subscription

Need 0.01306361 BTC

Bronze • Three Month C&C Subscription \$150 USD

- 250kb Unique EXE - Combo Encrypter/Decrypter
- Compatible with Windows XP to Windows 10
- You receive 100% of the ransom paid by the victims
- Supports Delayed Start, Mutex, and Task Manager Disabler
- Ransomware still works if you don't continue your C&C subscription
- Free support with active C&C subscription

Need 0.03265903 BTC

Silver • Six Month C&C Subscription \$250 USD

- 250kb Unique EXE - Combo Encrypter/Decrypter
- Compatible with Windows XP to Windows 10
- You receive 100% of the ransom paid by the victims
- Supports Delayed Start, Mutex, and Task Manager Disabler
- Ransomware still works if you don't continue your C&C subscription
- Free support with active C&C subscription

Need 0.05443172 BTC

Gold • One Year C&C Subscription \$400 USD

- 250kb Unique EXE - Combo Encrypter/Decrypter
- Compatible with Windows XP to Windows 10
- You receive 100% of the ransom paid by the victims
- Supports Delayed Start, Mutex, and Task Manager Disabler
- Ransomware still works if you don't continue your C&C subscription
- Free support with active C&C subscription

Need 0.08709076 BTC

Platinum • Three Year C&C Subscription \$650 USD

- 250kb Unique EXE - Combo Encrypter/Decrypter
- Compatible with Windows XP to Windows 10
- You receive 100% of the ransom paid by the victims
- Supports Delayed Start, Mutex, and Task Manager Disabler
- Ransomware still works if you don't continue your C&C subscription
- Free support with active C&C subscription

Need 0.14152248 BTC

## Features

- Packages are compiled with your Bitcoin and Email addresses so you are paid directly by your victim
  - Each package also supports Testnet mode, so you can test the ransomware in a virtual machine before distribution
- Packages utilize advanced polymorphic techniques to avoid over 90% of popular antivirus products

**Create the plan**







# **I. Table of Contents**

II.	Purpose .....
III.	Definitions .....
IV.	Roles & Responsibilities.....
V.	Stakeholders.....
VI.	Incident Assessment.....
VII.	Impact Criteria.....
VIII.	Scope Criteria .....
IX.	Threat Escalation Protocol .....
X.	Process Workflow.....
XI.	Response Procedures .....
XII.	Appendix .....

# Practice makes perfect

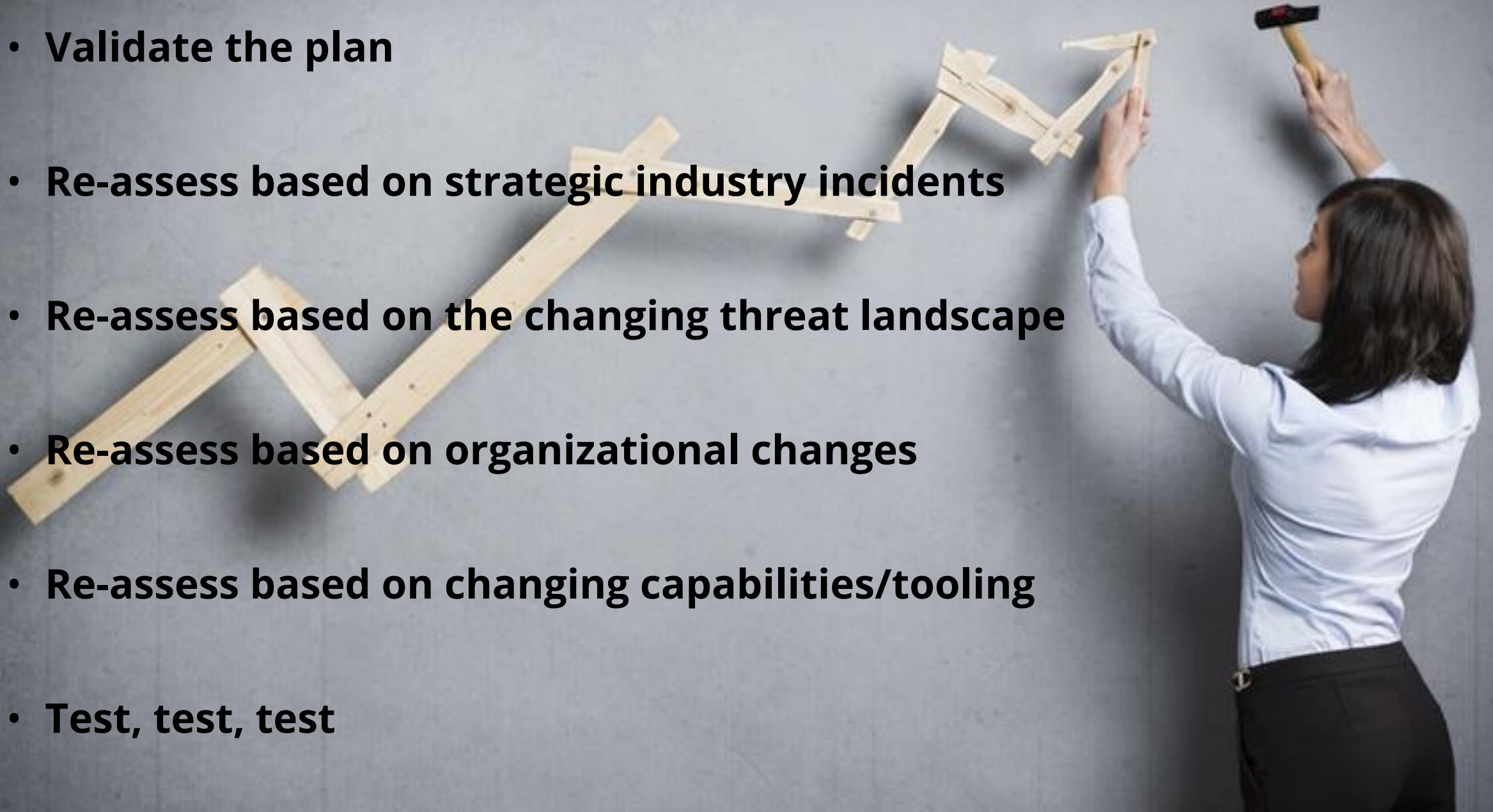
- Who should practice ?
- How to practice?





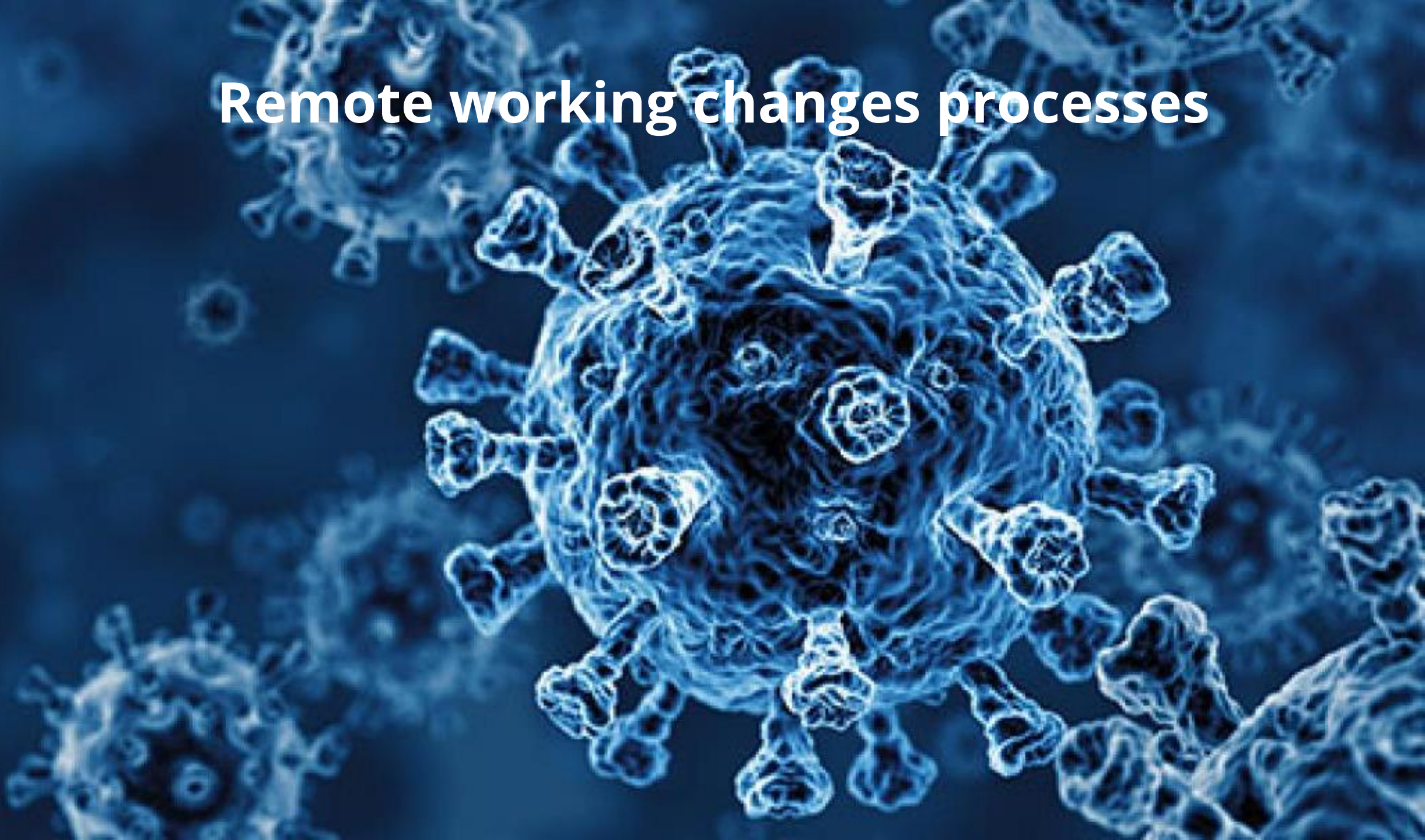
# Continuously improve

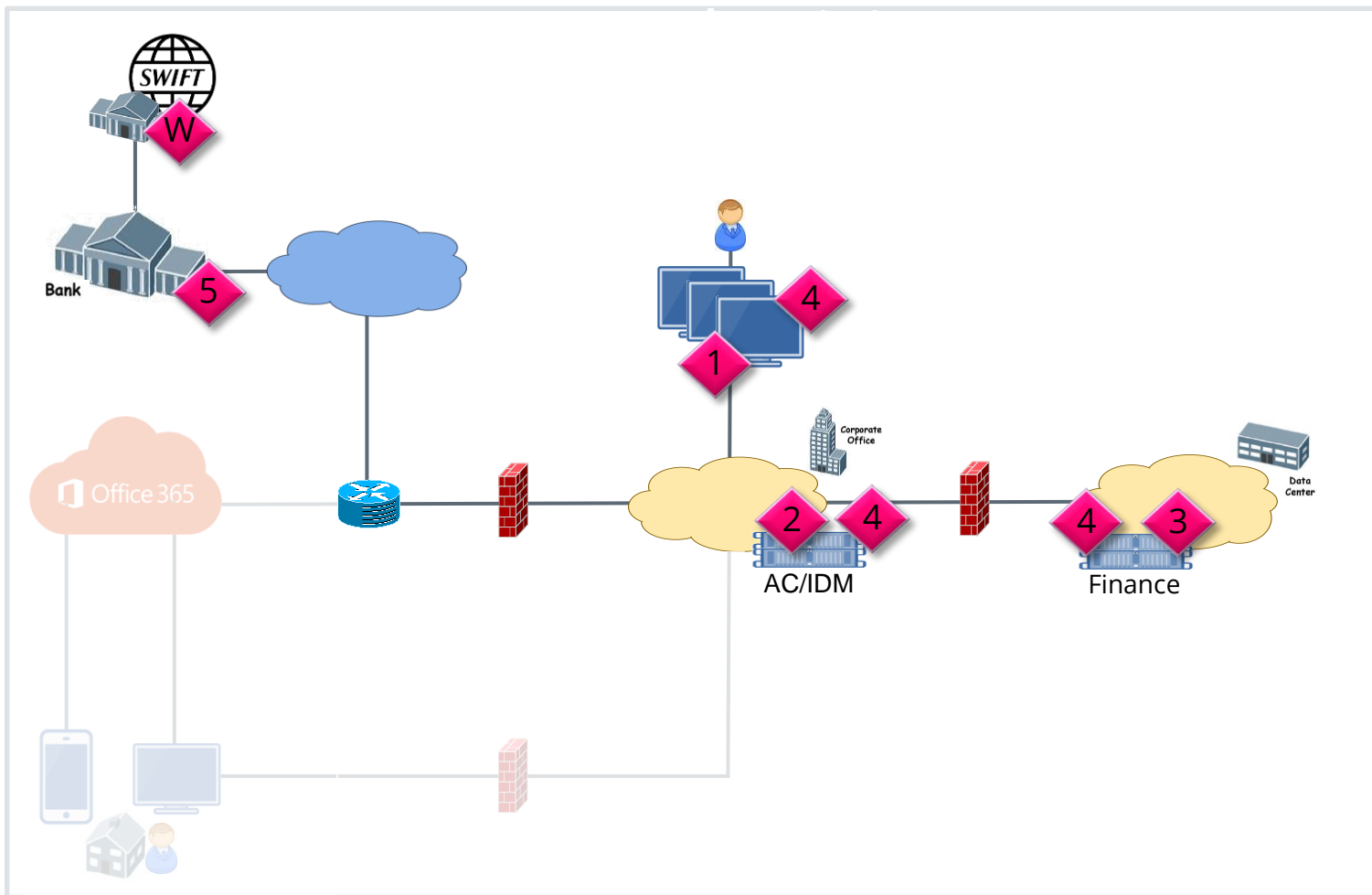
- **Validate the plan**
- **Re-assess based on strategic industry incidents**
- **Re-assess based on the changing threat landscape**
- **Re-assess based on organizational changes**
- **Re-assess based on changing capabilities/tooling**
- **Test, test, test**





**Remote working changes processes**





1 Login

2 Credential to the Financial Sys.

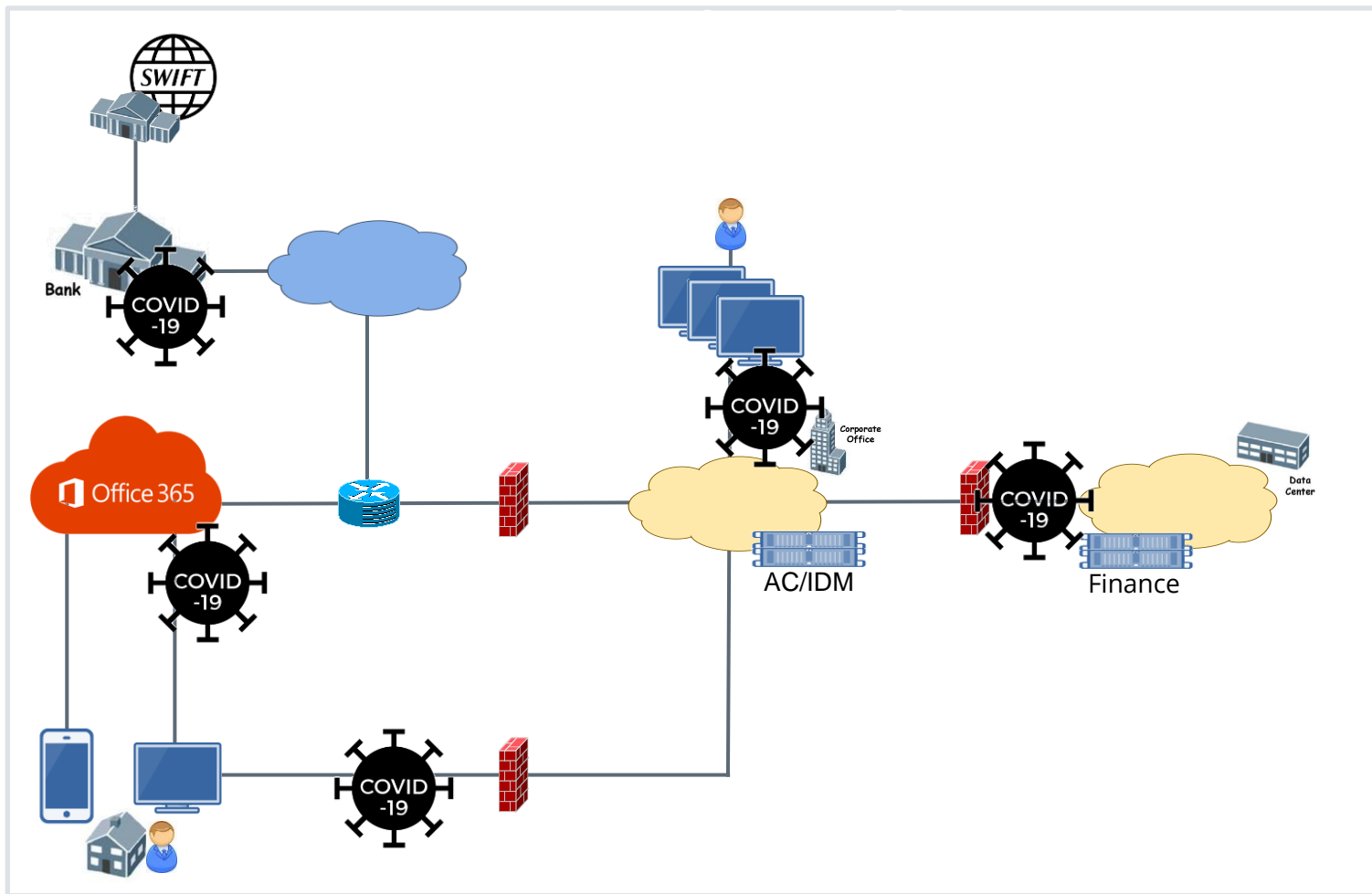
3 Generate a new Wire

4 Manager's approval (SoD)

5 Wire request sent

W Wire transfer





Offices closed



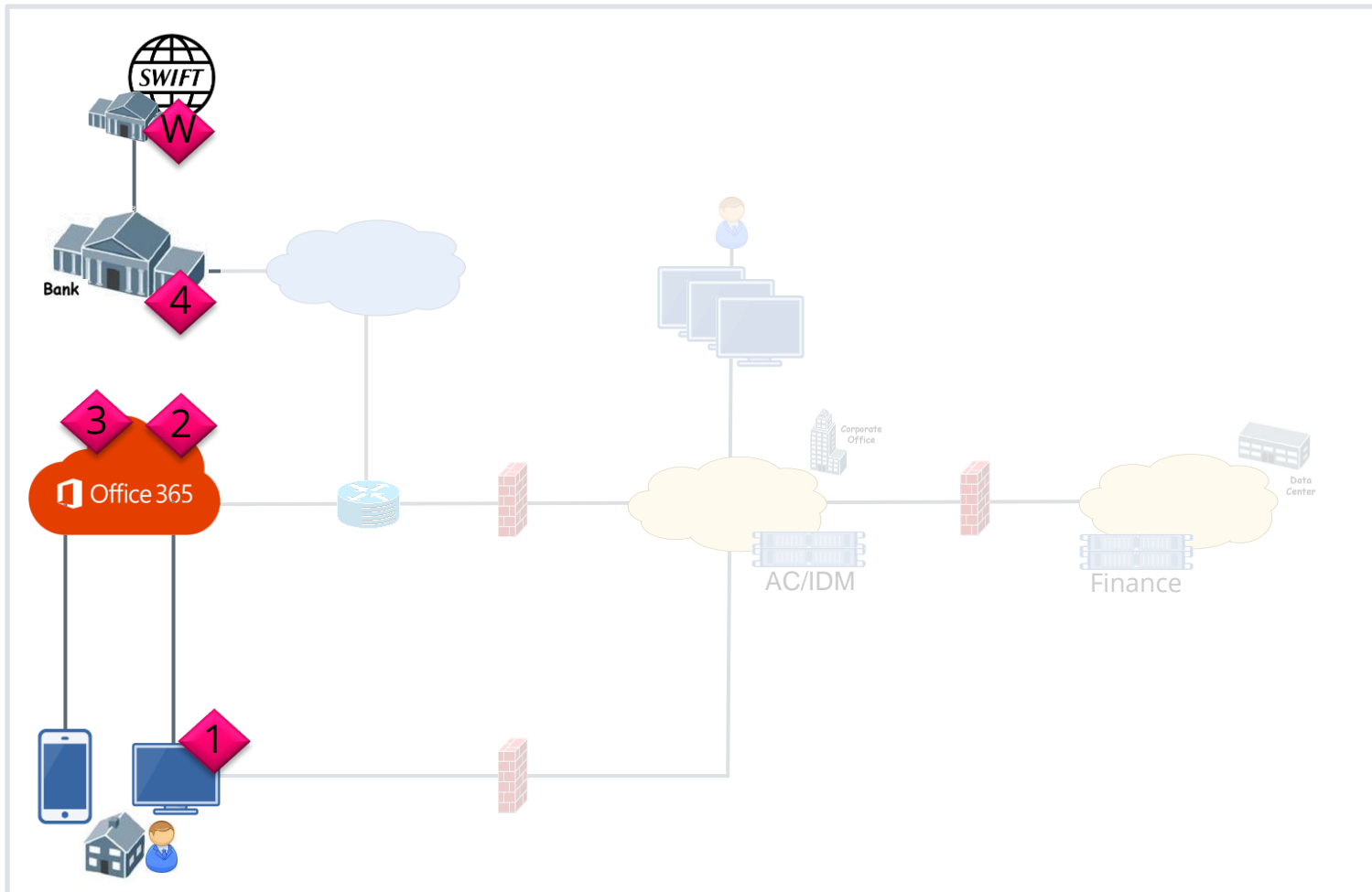
VPN access introduced new risks



Users utilized emails for core processes



Bank's employees working remote and ease their wire approval processes



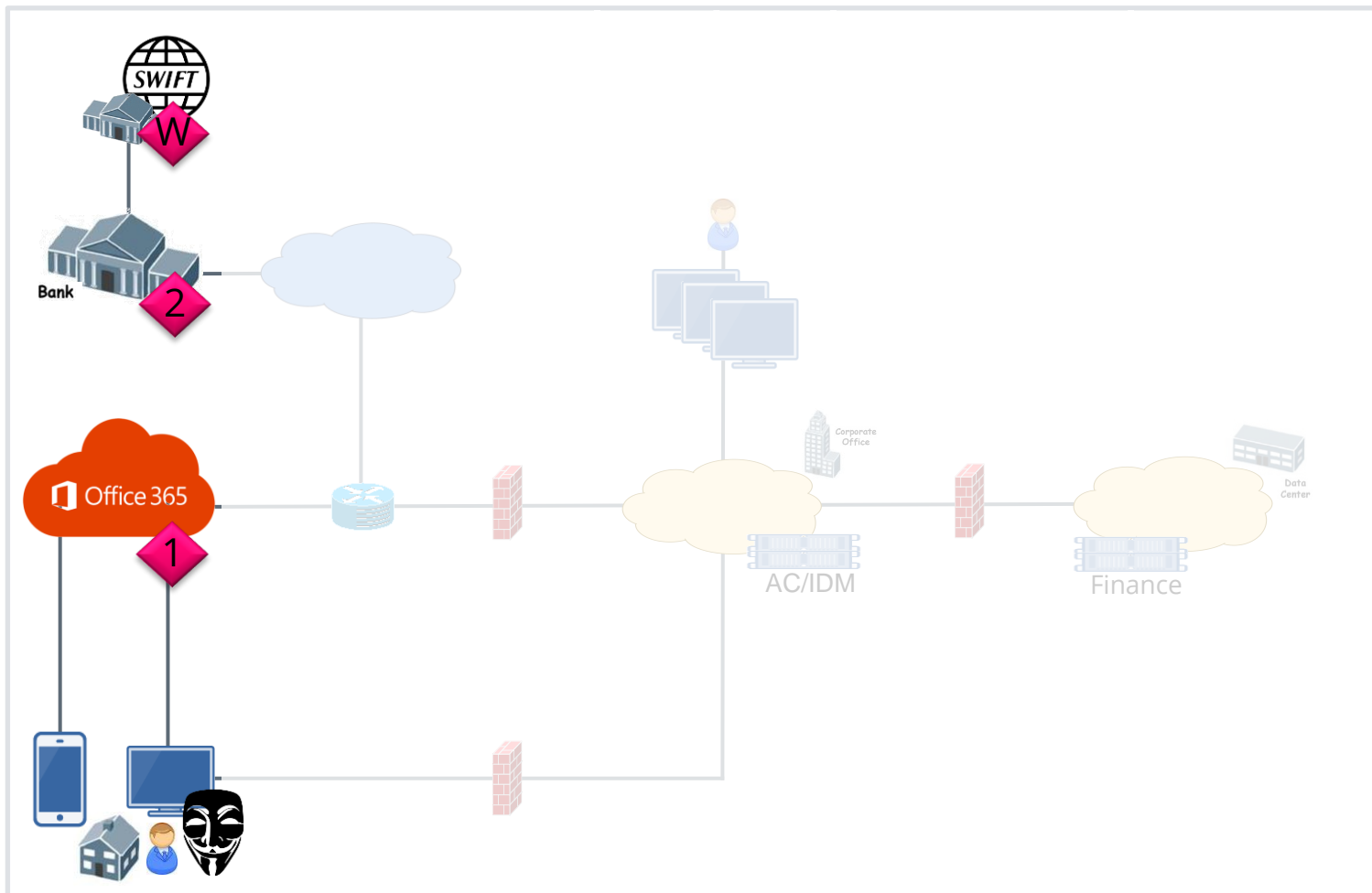
1 OWA

2 Wire request through email

3 Internal approvals through emails

4 Wire request sent

W Wire transfer



Credential Theft



Fraudulent Wire request though email, with fake approval processes text in the email body



Wire request email sent




Wire transfer



# Preparations !

- **Appropriate tools**
- **Excellent IR team**
- **Supporting processes & procedures.**



**BE PREPARED**

# Sometimes it's just not enough

The image shows a ransomware decryption website with a chat support window overlaid. The website text includes:

68610tek69-HOW-TO-DECRYPT.txt - Notepad

File Edit Format View Help

--=== Welcome. Again. ===--

[+] Whats Happen? [+]

Your files are encrypted  
By the way, everything

[+] What guarantees? [-]

Its just a business. We  
To check the ability of  
If you will not cooper

[+] How to get access [-]

You have two ways:

- 1) [Recommended] Using
  - a) Download and inst
  - b) Open our website:
- 2) If TOR blocked in yo
  - a) Open your any bro
  - b) Open our secondary

Warning: secondary web:

When you open our webs:  
Key:

```
9JpIghNjU8D2wxKv5VQL7T:
yJogTHsvHFTiC8XJoDvmPKI
Z7VpeXXnD6ebGdXTkJ3CCzi
aavqDxho6A4TukRMXkVd4ti
aFkZAA64V9zqFJrLsBv71W
mrFSZp069Sgajv01vV2tnil
UZaVoxhMZjz0S2ewWt0QN3I
M1Sc3JPue7ZABW0tNxfFqD:
```

How to restore the computer?

1 Enter the key here:

```
9JpIghNjU8D2wxKv5VQL7T:zqz3S7QfHa8MQu08BQEDoV1BAX5Jkhu1FAQ+Q072D
yJogTHsvHFTiC8XJoDvmPKIcs+nJoM91B+6E71FG7aOrV9Nexe3Qux21fCwS3K9R
Z7VpeXXnD6ebGdXTkJ3CCznVkiXIaQC48tekk2+qyzRmFg4z15EFAqg1ioWyTzVv
```

INSTRUCTIONS | **CHAT SUPPORT** | ABOUT US

Okay, so i consulted with my bosses, and we managed to find backups for a lot of our important files. The only one left encrypted that's actually important for us, is "GL\_Detailposting.M4T.lfeftvLd490s88". That's the most important, and the only file we need to decrypt. It's a 30MB file, and we aren't willing to pay the whole price for it. It's a bit extreme to pay 150,000 USD for a 30MB file, don't you think ?

We are however willing to pay a much lower price. What do you say ? What's the best discount we can get for a 30MB file ?

7 days ago

there will be no discount for you

7 days ago

Type your question here



# **IR plan cannot be an isolated effort**

- **All security initiatives must work together to facilitate cyber resilience**







**Thank you**



# Roles & Responsibilities

Legend:  
 R – Responsible  
 A – Accountable  
 C – Consulted  
 I – Informed

	End Users	Help Desk	MS SP/ Strategic Security Vendors	Cybersecurity	IT Operations	CISO	Legal	Human Resources	Public Relations	Senior Management	External (e.g. Law Enforcement)
<b>Detection &amp; Analysis</b>											
Report a suspected incident, such as a service disruption, a suspicious email, or an unusual endpoint behavior.	A	R	C	C	C	I	-	-	-	-	-
Open a help desk ticket	I	R	R	I	-	A	-	-	-	-	-
Gather answers to incident-related questions.	C	A	-	-	-	A	-	-	-	-	-
Perform indicator of compromise (IoC) search (firewall, IDP, email gateway, SIEM, logs, etc.).	-	C	R	R	C	A	-	-	-	-	-
Determine what, if any, systems or devices were compromised (e.g. end-user devices, servers, applications).	C	C	C	R	R	A	-	-	-	-	-
Assess the impact to servers, applications, storage, or other systems.	-	C	C	R	C	A	-	-	-	I	-
Determine the scope/breadth of the incident.	-	C	C	R	C	A	-	-	-	I	-



Table 3. Threat Escalation Protocol

Threat Escalation Protocol (TEP)			
Impact	Scope		
	High	Medium	Low
High	Tier 1	Tier 1	Tier 2
Medium	Tier 1	Tier 2	Tier 2
Low	Tier 2	Tier 2	Tier 3

Threat Escalation Protocol (TEP)	Criteria	Stakeholders
TEP Tier 1	<ul style="list-style-type: none"><li>• High impact, high scope</li><li>• High impact, medium scope</li><li>• Medium impact, high scope</li></ul>	<ul style="list-style-type: none"><li>• End User</li><li>• Help Desk</li><li>• Cybersecurity*</li><li>• IT Operations</li><li>• CISO</li><li>• Legal, HR, Customer Service</li><li>• Senior Management</li><li>• External Third Parties</li></ul>
TEP Tier 2	<ul style="list-style-type: none"><li>• High impact, low scope</li><li>• Medium impact, medium scope</li><li>• Medium impact, low scope</li><li>• Low impact, high scope</li><li>• Low impact, medium scope</li></ul>	<ul style="list-style-type: none"><li>• End User</li><li>• Help Desk</li><li>• Cybersecurity*</li><li>• IT Operations</li><li>• CISO</li></ul>
TEP Tier 3	<ul style="list-style-type: none"><li>• Low impact, medium scope</li><li>• Low impact, low scope</li></ul>	<ul style="list-style-type: none"><li>• End User</li><li>• Help Desk</li><li>• Cybersecurity*</li></ul>