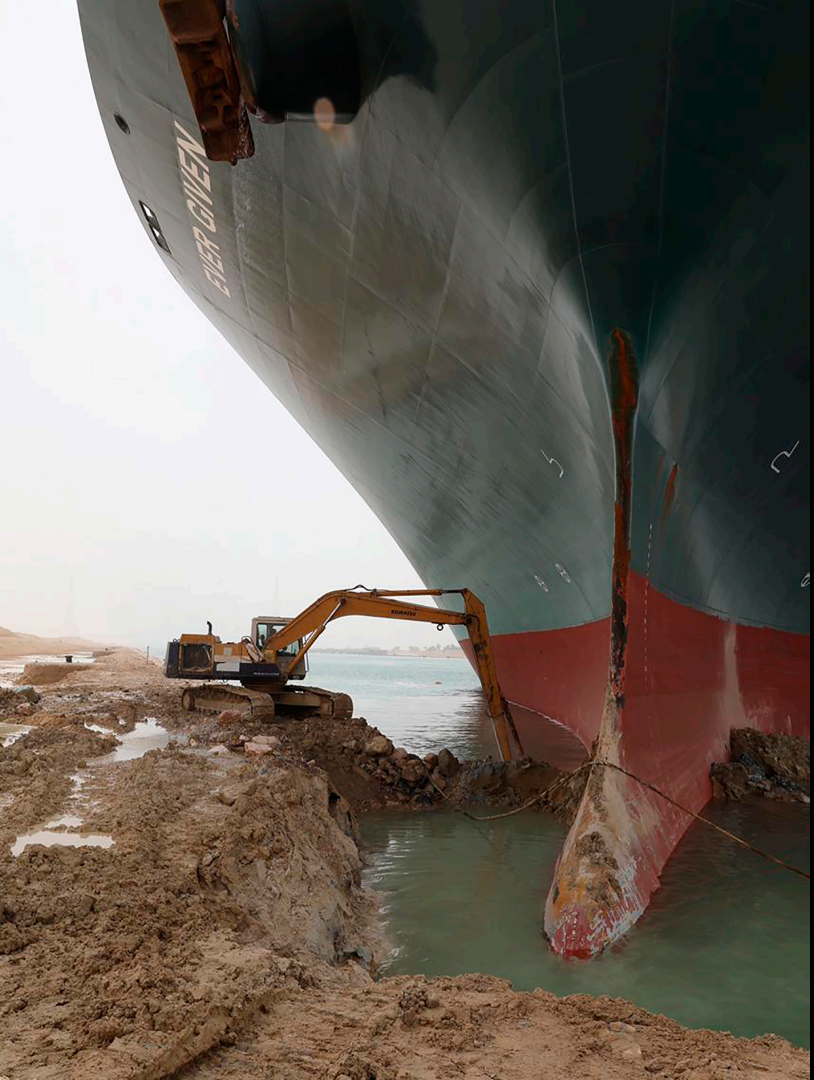
proofpoint

Break the attack chain with people-centric security.

Adenike Cosgrove

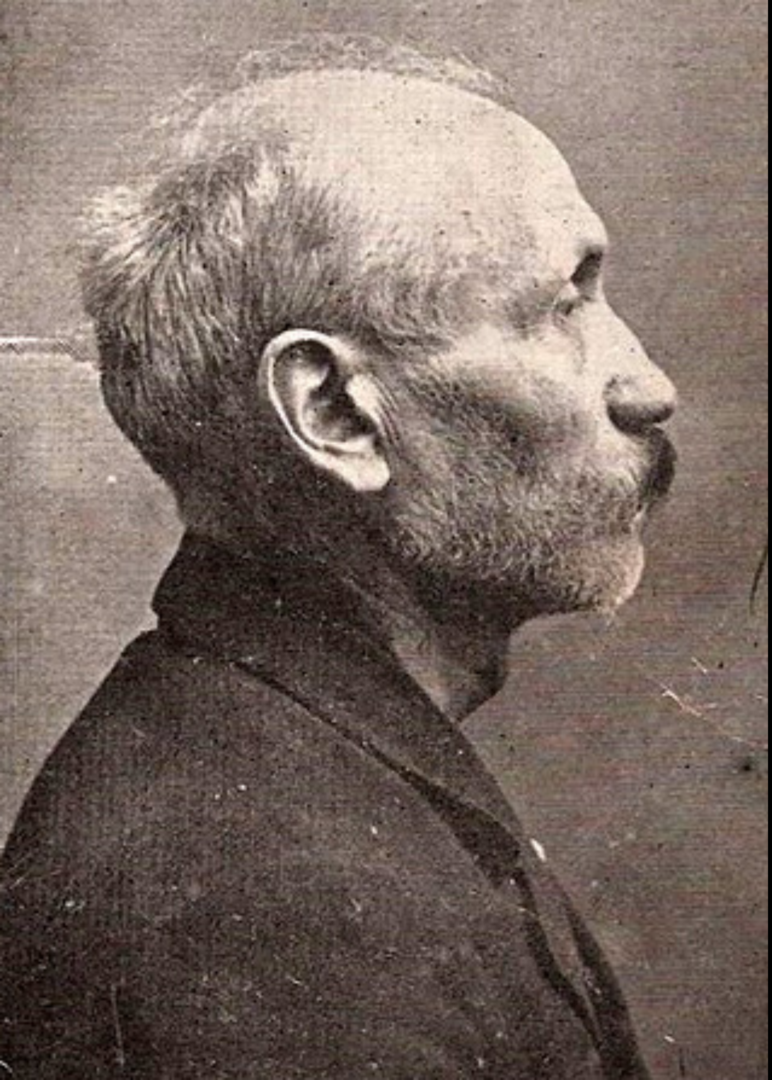
VP, Cybersecurity Strategy



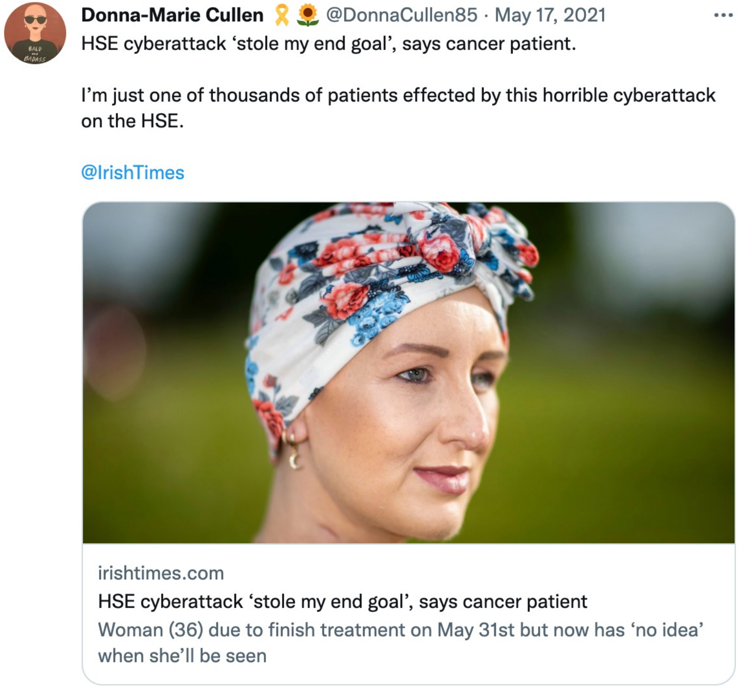
> “Egypt’s canal chief says human error could be behind ship’s grounding.”

proofpoint.

STADT-KAFFEE
STADT-KAFFEE
FFEE
STADT-KAFFEE
oria
EMIL RÖGENER
Waldorf-Astoria Cigarettes
6
Café Kröpcke.



“Friedrich Wilhelm Voigt masqueraded as a military officer, rounded up soldiers, and ‘confiscated’ 4,000 marks from a municipal treasury.”



Donna-Marie Cullen 🎗️🌻 @DonnaCullen85 · May 17, 2021

HSE cyberattack ‘stole my end goal’, says cancer patient.

I’m just one of thousands of patients effected by this horrible cyberattack on the HSE.

@IrishTimes

irishtimes.com

HSE cyberattack ‘stole my end goal’, says cancer patient

Woman (36) due to finish treatment on May 31st but now has ‘no idea’ when she’ll be seen

“I got a call at lunchtime and was told that my radiation wouldn't be going ahead because of the cyber-attack.”

proofpoint

It started with a phish

Anatomy of the ransomware (or BEC, or data theft) attack

Initial access

Attacker looks for a way into the organisation

18 March 2021
User opened malicious Microsoft Excel file attached to a phishing email sent on 16 March 2021.

Consolidation & preparation

Attacker attempts to gain access to critical devices and server admin

18 March 2021 – 14 May 2021
Attacker operated in network over eight-week period.

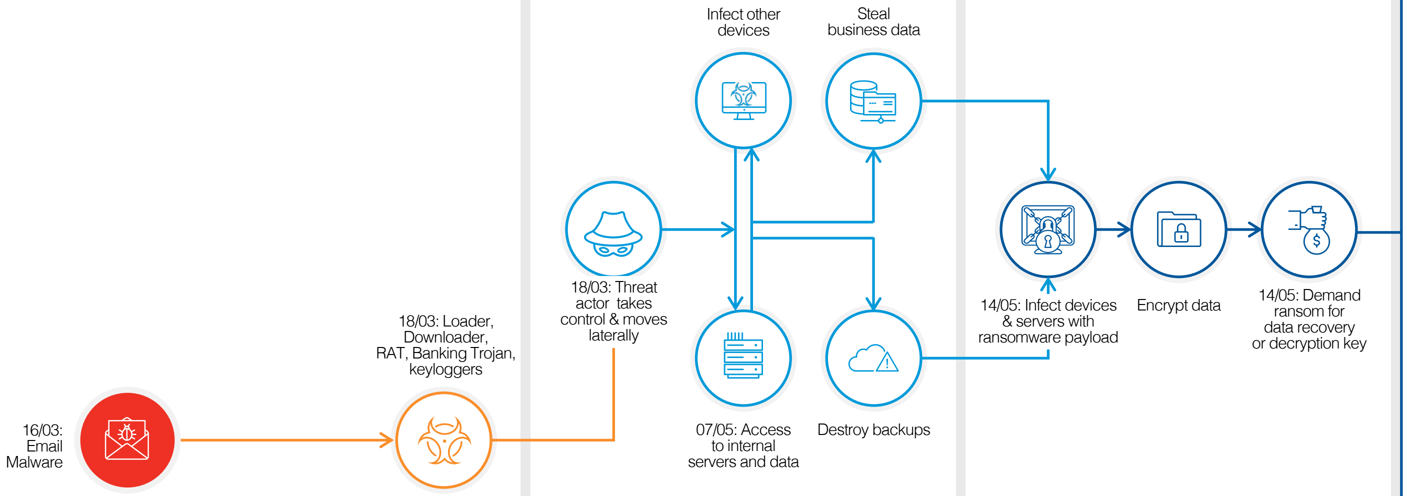
Ransomware launch

Once all systems identified, infected, and information collected, criminal then sends ransomware payload

14 May 2021
Detonation of Conti ransomware which caused widespread IT disruption.

Impact on target

Attacker steals and encrypts data, then demands ransom



16/03: Email Malware

18/03: Loader, Downloader, RAT, Banking Trojan, keyloggers

18/03: Threat actor takes control & moves laterally

Infect other devices

Steal business data

07/05: Access to internal servers and data

Destroy backups

14/05: Infect devices & servers with ransomware payload

Encrypt data

14/05: Demand ransom for data recovery or decryption key

Customer notifications

Disclosure of information on darkweb

Customer loss/ loss of sales

Reputational harm/ bad PR

Operational downtime

Response and remediation costs

Financial loss due to ransom payments

"For me it was the worry. If there was even a minute chance of a crumb of this cancer left in my head, that it would just start to multiply, and my radiation plan would need to be completely revised."

“We got into your network through phishing. The email with the malicious attachment was opened by an employee... the user is asked to include the document's macro to display the content.

#Solution: Make it impossible to perform such an attack!

#How? You should figure it out for yourself…”

Systemic risk is people-centric risk.

DBIR

Data Breach Investigations Report

85% of data breaches involved a human element, just 3% involved a technical vulnerability.

verizon

75% of ransomware attacks start with email.

paloalto NETWORKS

95% of security breaches are human related.

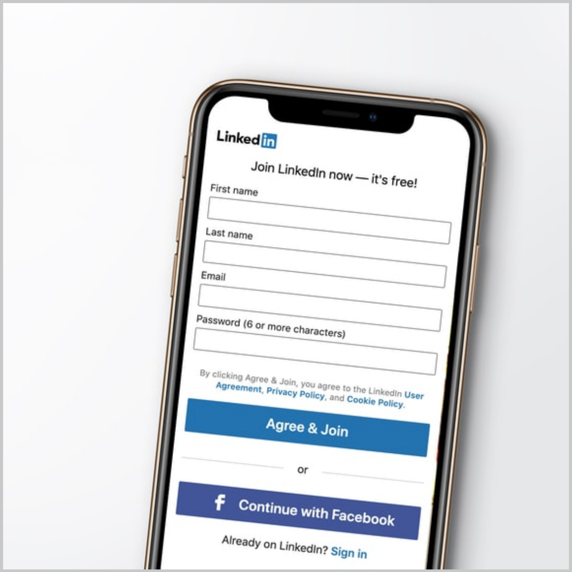
WORLD ECONOMIC FORUM

> “Had we known that what was true nine years ago would still be true today, we could have saved some time by just copying and pasting some text.
>
> Oh well, maybe in another nine years things will change for the better.”

verizon✓ DBIR

Attackers don’t hack in… they log in

RUNNING ATTACKER’S CODE FOR THEM



Linkedin

Join LinkedIn now — it's free!

First name

Last name

Email

Password (6 or more characters)

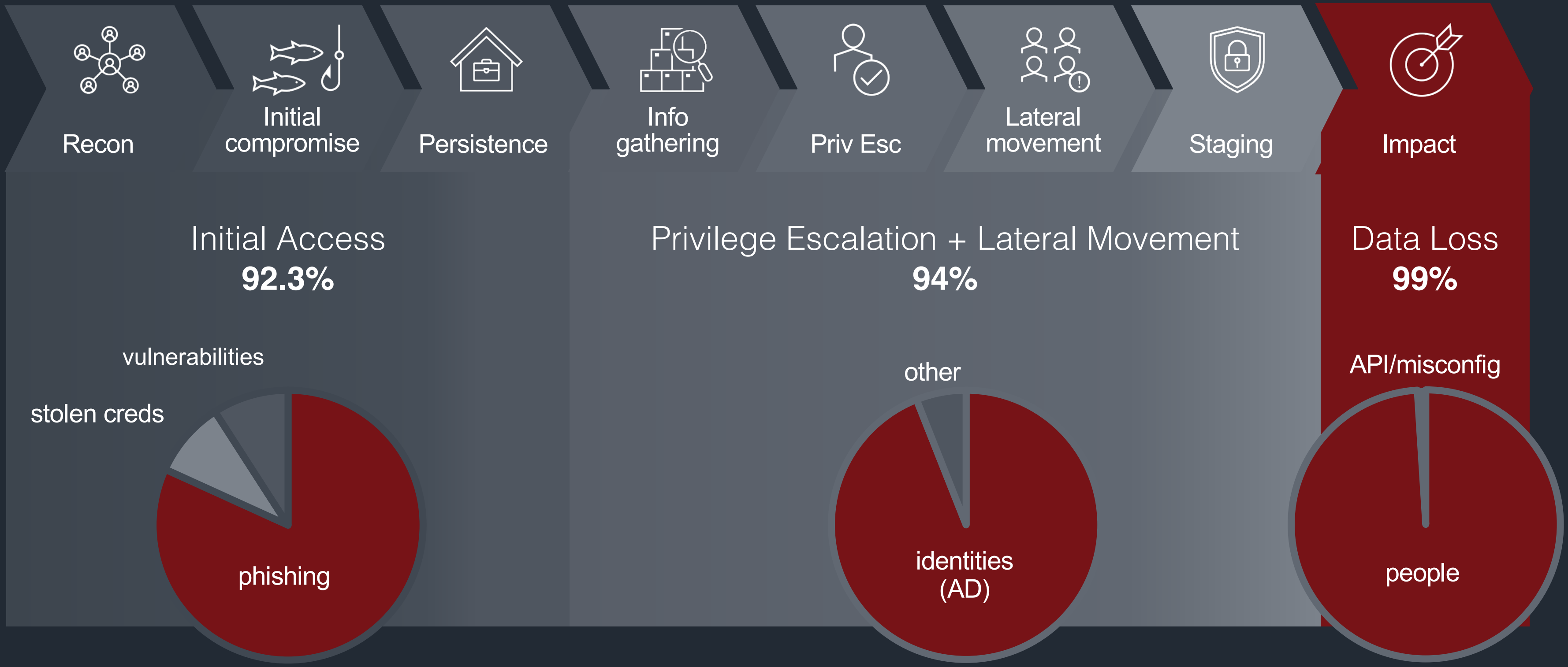
By clicking Agree & Join, you agree to the LinkedIn User Agreement, Privacy Policy, and Cookie Policy.

Already on LinkedIn? Sign in

HANDING OVER CREDENTIALS TO THEM

TRANSFER FUNDS OR DATA TO THEM

And they log in with standardized tactics



Recon

Initial compromise

Persistence

Info gathering

Priv Esc

Lateral movement

Staging

Impact

Initial Access
92.3%

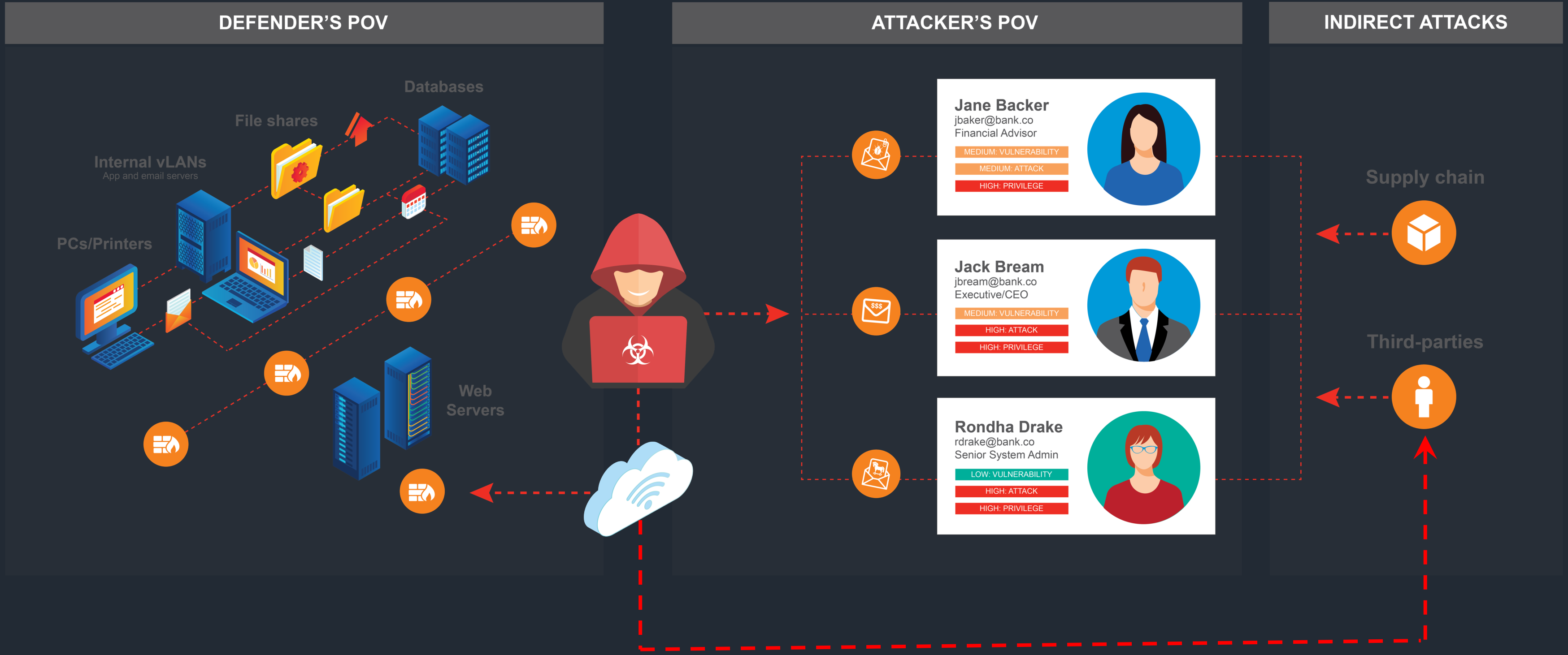
Privilege Escalation + Lateral Movement
94%

Data Loss
99%

Sources: DFIR Report 2022 Year in Review, 2022 Verizon DBIR

The human has always been the perimeter.

But have we changed our focus?



DEFENDER’S POV

ATTACKER’S POV

INDIRECT ATTACKS

Jane Backer
jbaker@bank.co
Financial Advisor
MEDIUM: VULNERABILITY
MEDIUM: ATTACK
HIGH: PRIVILEGE

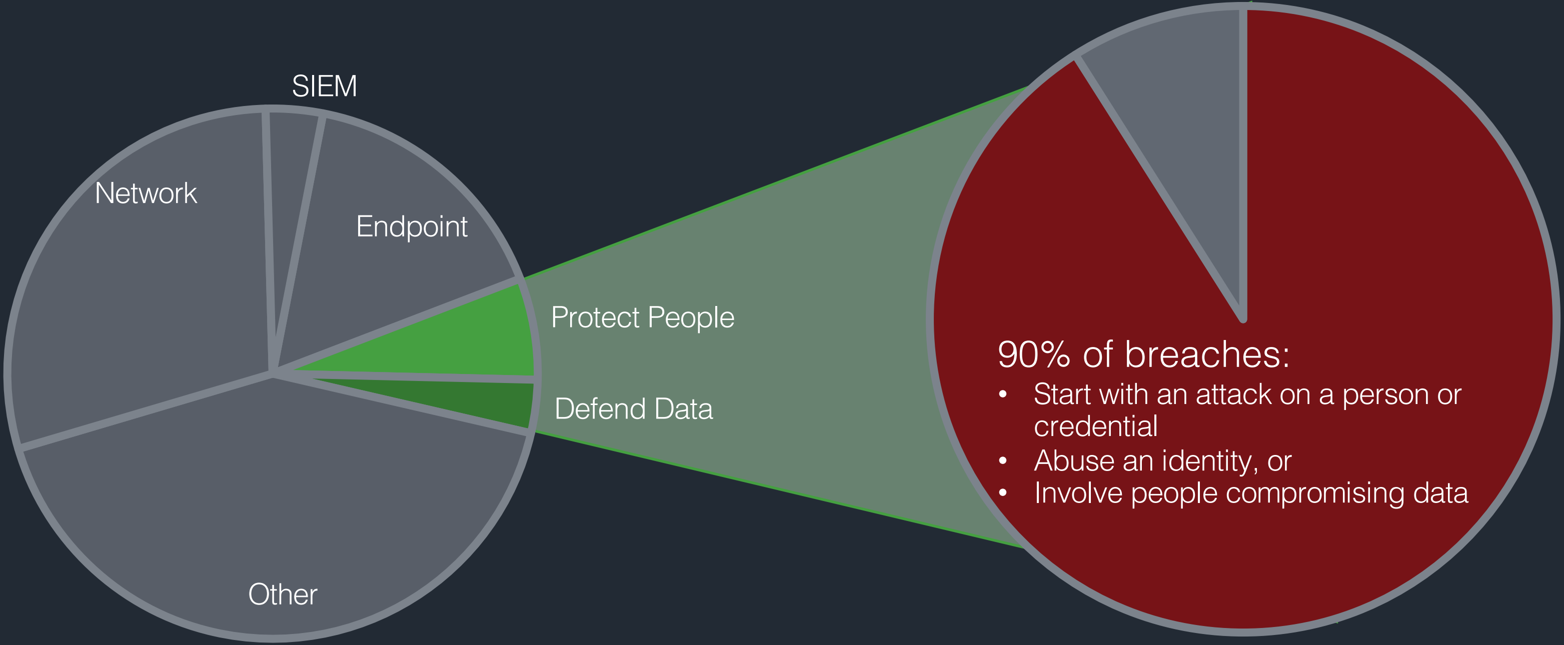
Jack Bream
jbream@bank.co
Executive/CEO
MEDIUM: VULNERABILITY
HIGH: ATTACK
HIGH: PRIVILEGE

Rondha Drake
rdrake@bank.co
Senior System Admin
LOW: VULNERABILITY
HIGH: ATTACK
HIGH: PRIVILEGE

Risks focused on people… defenders didn’t

2022 security spending:
<9% on protecting people

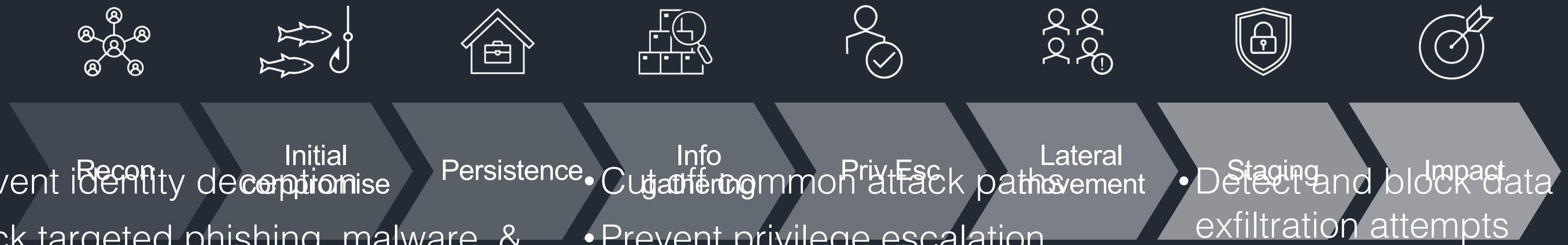
2022 security breaches:
>90% people-centric



90% of breaches:

- Start with an attack on a person or credential
- Abuse an identity, or
- Involve people compromising data

Breaking the links in the attack chain



- Prevent identity deception
- Block targeted phishing, malware, & social engineering attacks
- Detect + respond to cloud account takeover
- Build user resilience
- Identify compromised suppliers

Proofpoint **Aegis**

- Cut off common attack paths
- Prevent privilege escalation
- Detect lateral movement

Proofpoint **Identity Threat Detection + Response**

- Detect and block data exfiltration attempts
- Gain insight into risky user behaviour

Proofpoint **Sigma**

Answering the questions that matter most

AXIS:

Adversaries

Who are they and what do they want?

How do they operate?

Who else have they attacked?

AXIS:

People

Who is attacked?

Who is risky?

Who has privilege?

AXIS:

Data

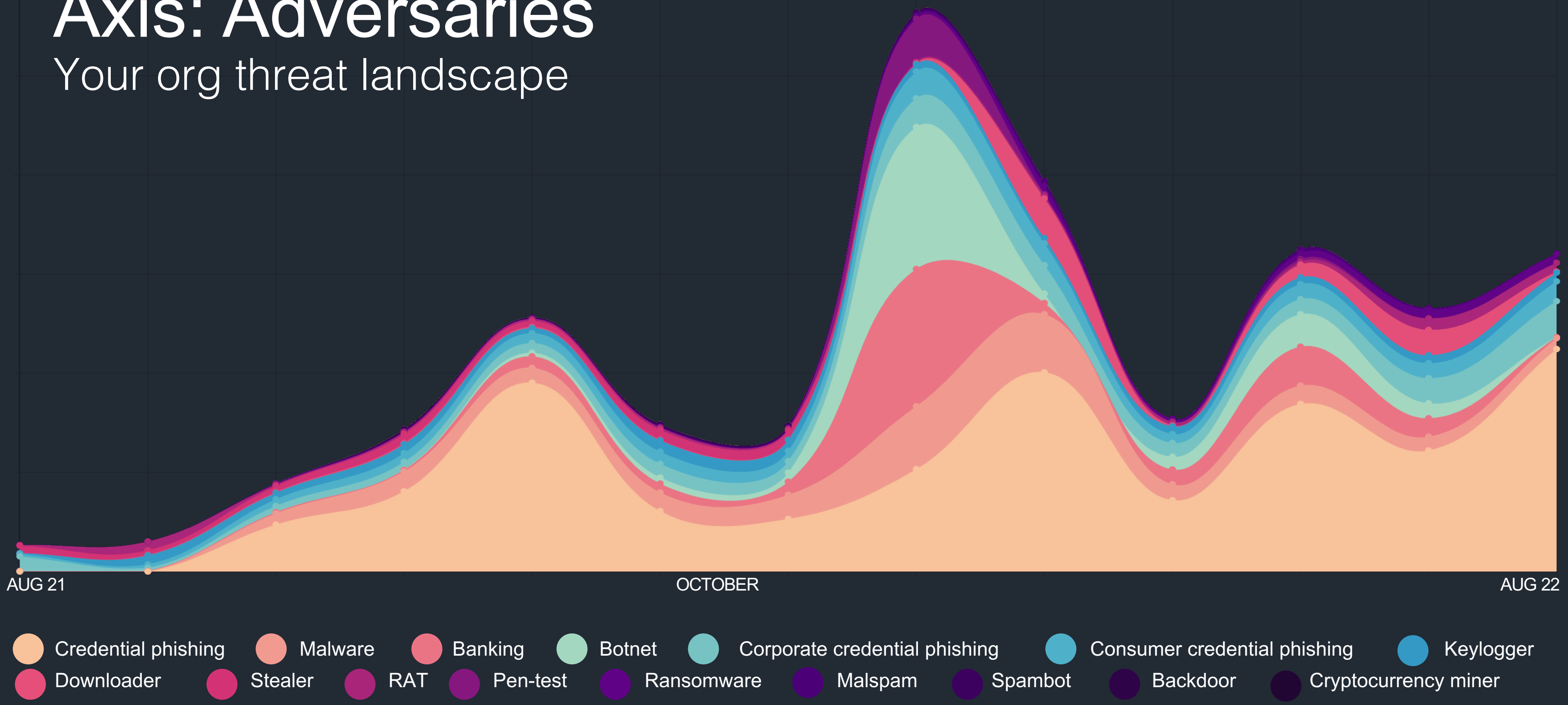
Who has access?

Is it sensitive?

Is it moving or stored in a risky way?

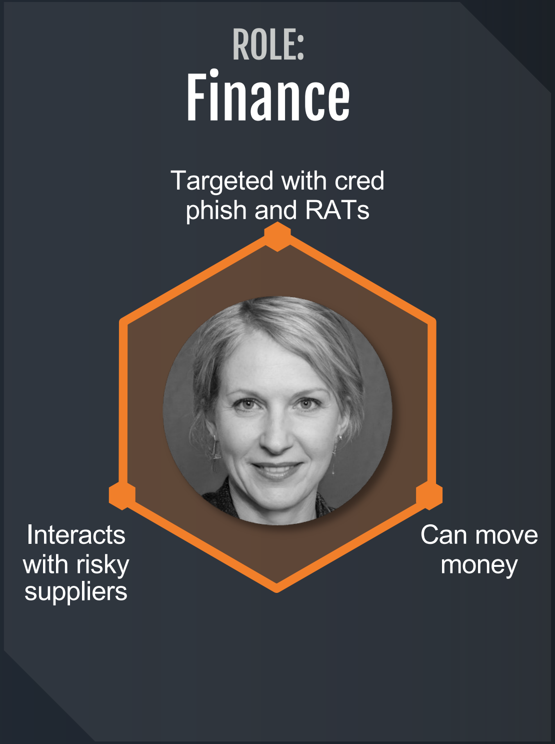
Axis: Adversaries

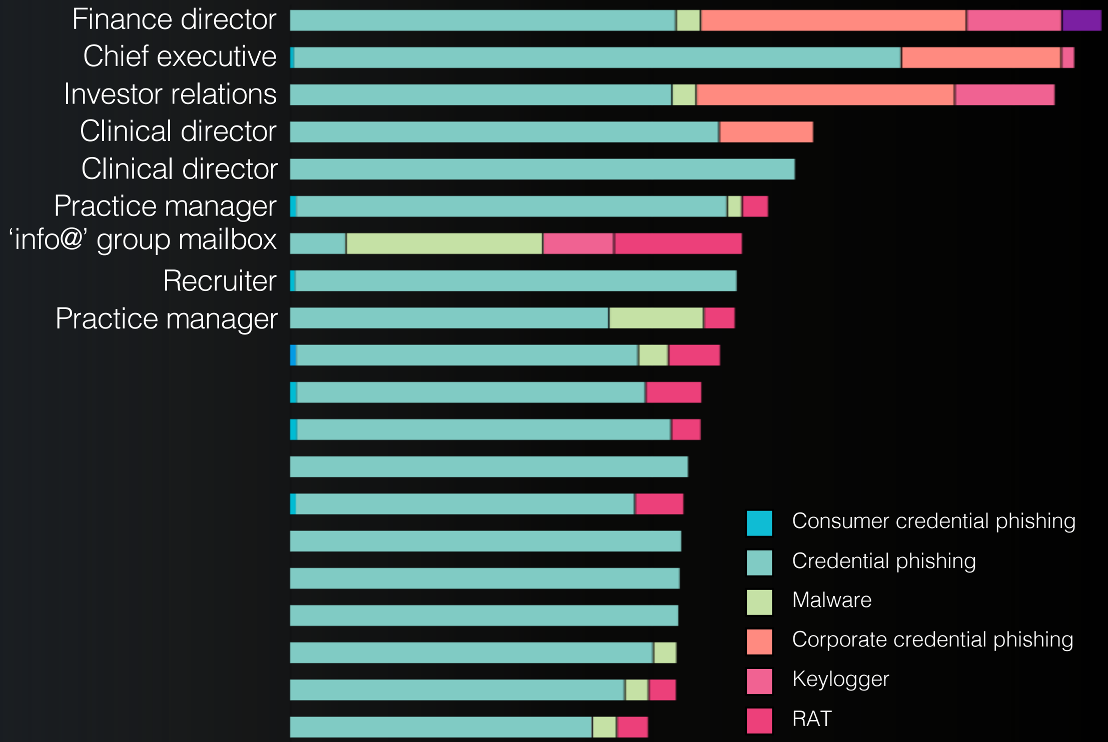
Your org threat landscape



Axis: People

People are different.... but targetable

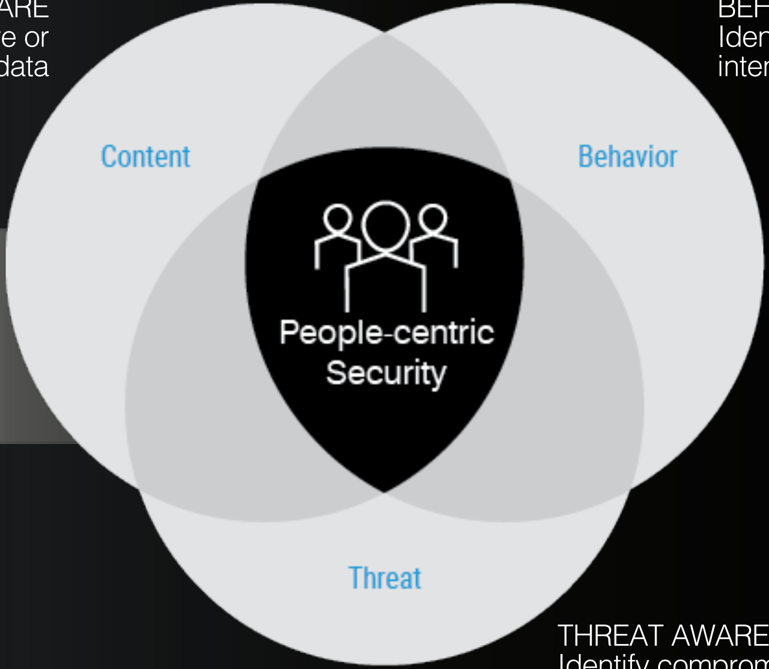

ROLE:
Finance
Targeted with cred phish and RATs
Interacts with risky suppliers
Can move money



Axis: Data

15 patterns cover 95%+ of data loss incidents

CARELESS USER
COMPROMISED USER
MALICIOUS USER



CONTENT AWARE
Identify sensitive or regulated data

BEHAVIOUR AWARE
Identify user activity, intent & context

THREAT AWARE
Identify compromised users & accounts with advanced threat intelligence

Axis: Data

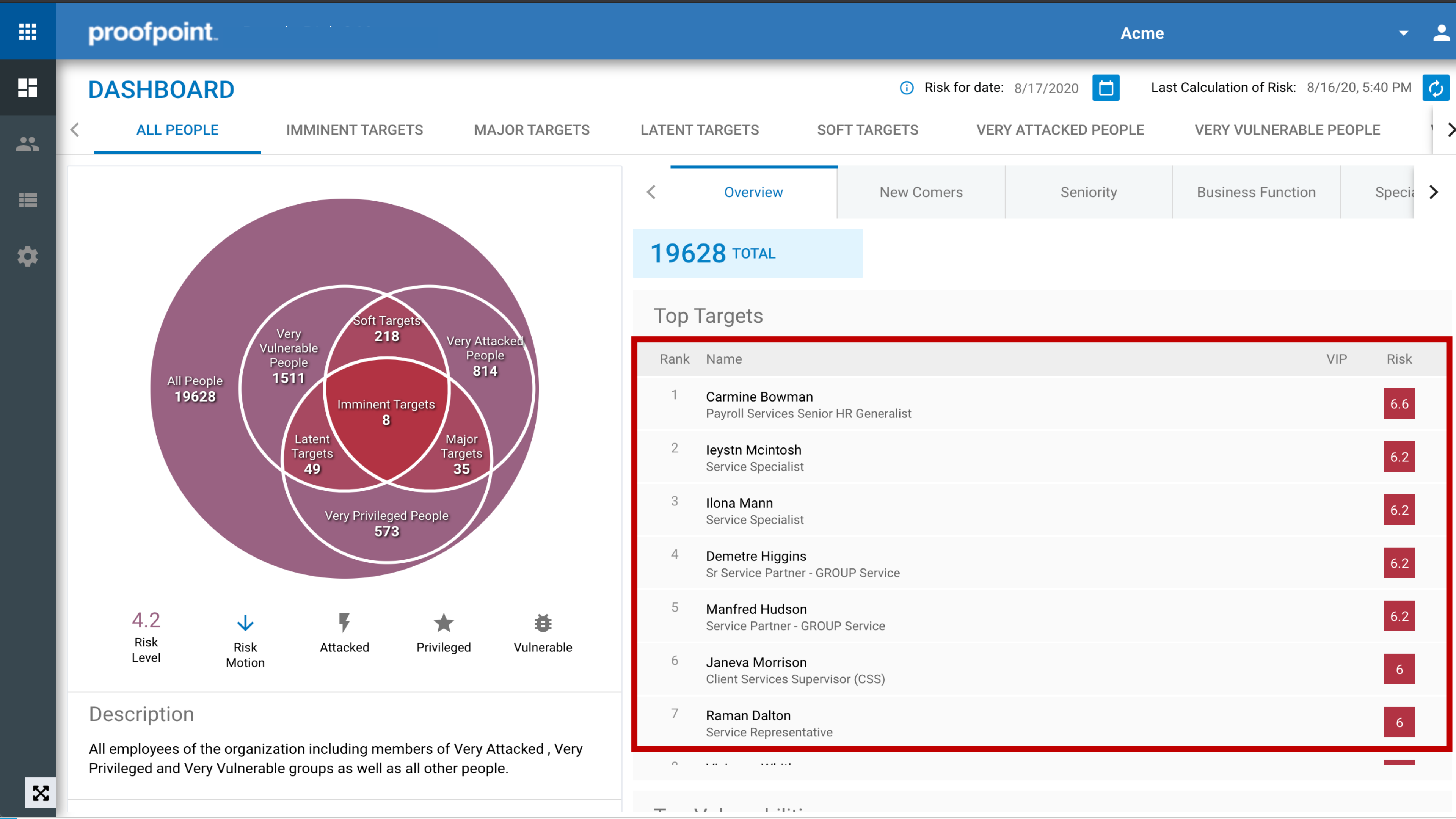
15 patterns cover 95%+ of data loss incidents

CARELESS USER

COMPROMISED USER

MALICIOUS USER

ACCESS	MANIPULATION	EXFILTRATION
Sync/copy cloud file stores	Change file name	Copy to personal cloud storage
Search/copy from file shares	Encrypt file	Share with personal / burner account
Copy structured data from thick client apps	Change file extension	Email to personal / burner account
Export data from web interfaces	Add to archive or compress file	Copy from cloud to unmanaged device
	Create multi-part archive	Copy to USB / external hard drive / AirDrop
		Print



DASHBOARD

Risk for date: 8/17/2020

Last Calculation of Risk: 8/16/20, 5:40 PM

19628 TOTAL

Top Targets

Rank	Name	VIP	Risk
1	Carmine Bowman Payroll Services Senior HR Generalist		6.6
2	Ieystn Mcintosh Service Specialist		6.2
3	Ilona Mann Service Specialist		6.2
4	Demetre Higgins Sr Service Partner - GROUP Service		6.2
5	Manfred Hudson Service Partner - GROUP Service		6.2
6	Janeva Morrison Client Services Supervisor (CSS)		6
7	Raman Dalton Service Representative		6

Description

All employees of the organization including members of Very Attacked , Very Privileged and Very Vulnerable groups as well as all other people.

Adaptive controls that protect people

ROLE:

Finance

Block impostor attacks with ML

Flag risky suppliers with tags

Train on BEC threats

ROLE:

Research Scientist

Web isolation to preserve privacy

Protect cloud collaboration with web, endpoint DLP

Deliver custom training on campaigns targeting intellectual property

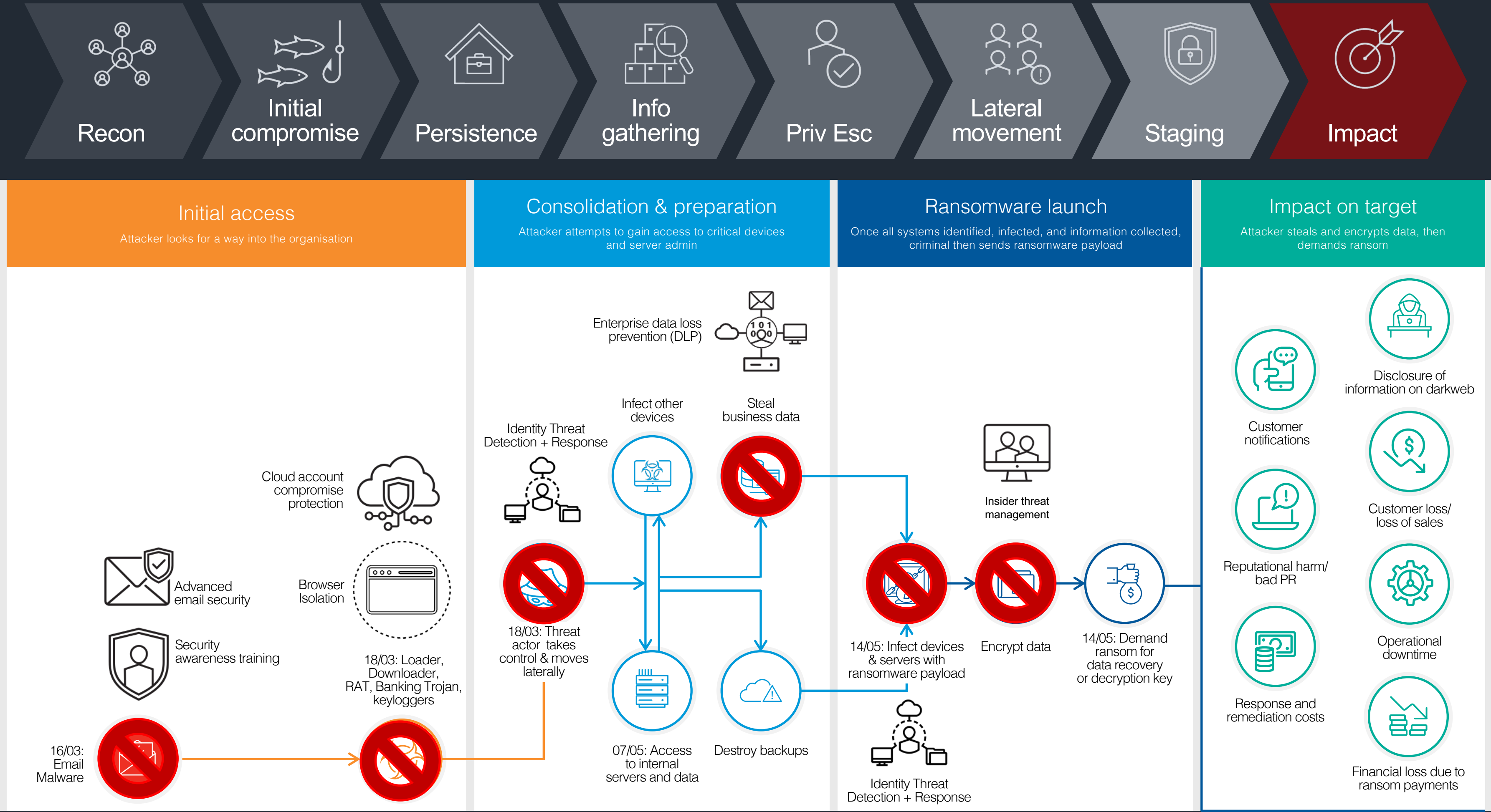
ROLE:

Support

Isolate all links to shared alias so clicks do no harm

Use ITM to protect customer data

Train on data handling



Recon | Initial compromise | Persistence | Info gathering | Priv Esc | Lateral movement | Staging | Impact

Initial access

Attacker looks for a way into the organisation

Cloud account compromise protection

Advanced email security

Browser Isolation

Security awareness training

16/03: Email Malware

18/03: Loader, Downloader, RAT, Banking Trojan, keyloggers

Consolidation & preparation

Attacker attempts to gain access to critical devices and server admin

Enterprise data loss prevention (DLP)

Identity Threat Detection + Response

Infect other devices

Steal business data

18/03: Threat actor takes control & moves laterally

07/05: Access to internal servers and data

Destroy backups

Ransomware launch

Once all systems identified, infected, and information collected, criminal then sends ransomware payload

Insider threat management

14/05: Infect devices & servers with ransomware payload

Encrypt data

14/05: Demand ransom for data recovery or decryption key

Identity Threat Detection + Response

Impact on target

Attacker steals and encrypts data, then demands ransom

Customer notifications

Disclosure of information on darkweb

Reputational harm/ bad PR

Customer loss/ loss of sales

Response and remediation costs

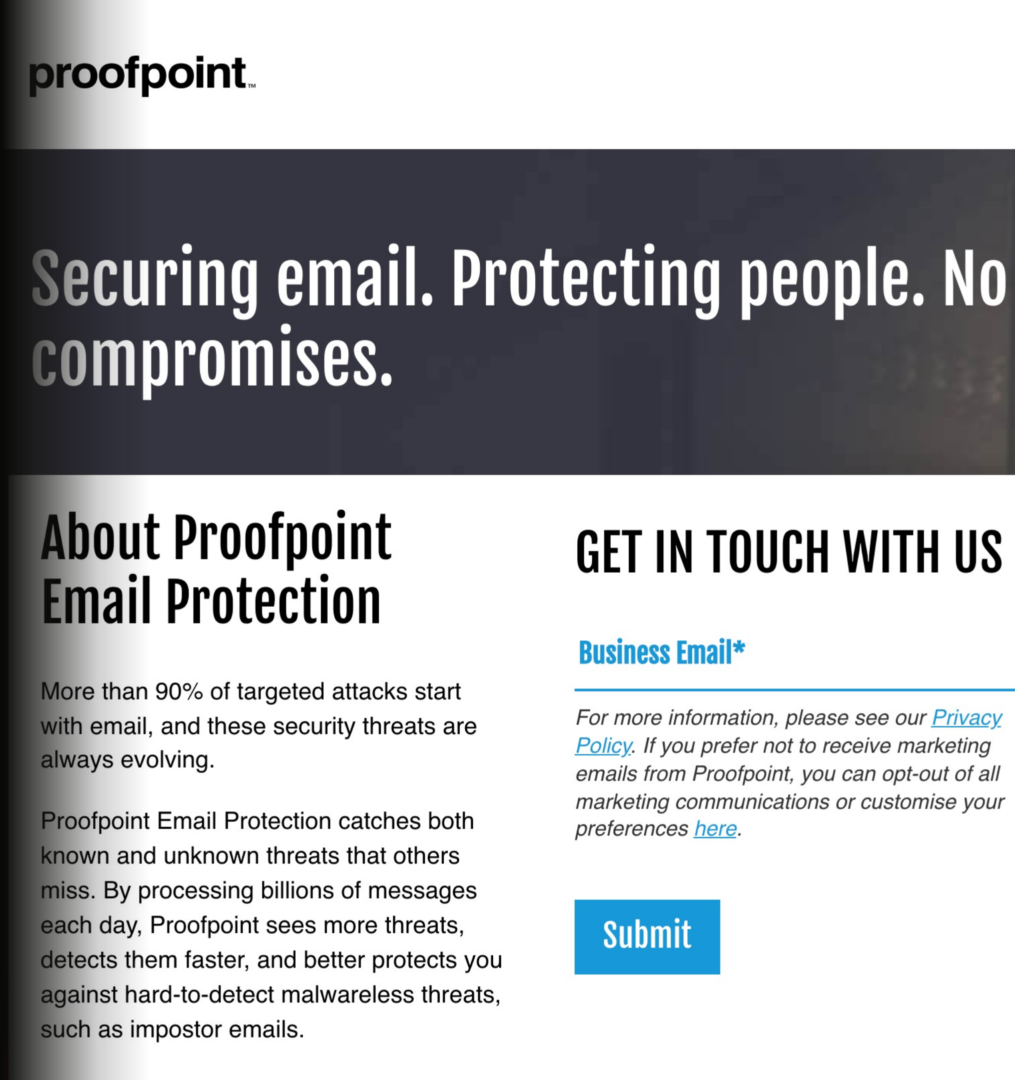
Operational downtime

Financial loss due to ransom payments

Learn more

Uncover your Very Attacked People

go.proofpoint.com/en-email-security-get-in-touch.html



Securing email. Protecting people. No compromises.

About Proofpoint Email Protection

More than 90% of targeted attacks start with email, and these security threats are always evolving.

Proofpoint Email Protection catches both known and unknown threats that others miss. By processing billions of messages each day, Proofpoint sees more threats, detects them faster, and better protects you against hard-to-detect malwareless threats, such as impostor emails.

GET IN TOUCH WITH US

Business Email*

For more information, please see our Privacy Policy. If you prefer not to receive marketing emails from Proofpoint, you can opt-out of all marketing communications or customise your preferences here.

proofpoint®