
THE BAD, BETTER, AND BEST
SOCIAL ENGINEERING INCIDENT RESPONSE
ROB RAGAN
@SWEEPTHATLEG
ALEX DEFREESE
@LUNARCA_

Hello!

We are Rob and Alex

Security consultants at Bishop Fox.

We help organizations secure their networks, applications, and people.

1

What are we talking about here?

1

What are we talking about here?

This talk explores the challenges of responding to social engineering incidents and improving defense.

1

What are we talking about here?

This talk explores the challenges of responding to social engineering incidents and improving defense.

Does your organization have a social engineering-specific response plan?

Bad

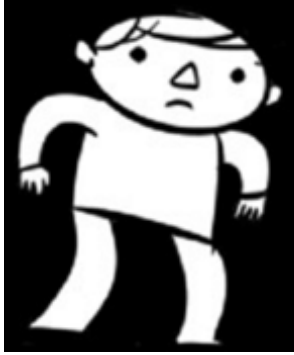
The worst incident responses

Phone Social Engineering

International News Agency

- Impersonate an employee
- Call helpdesk for password reset
- Gain access to internal network and resources

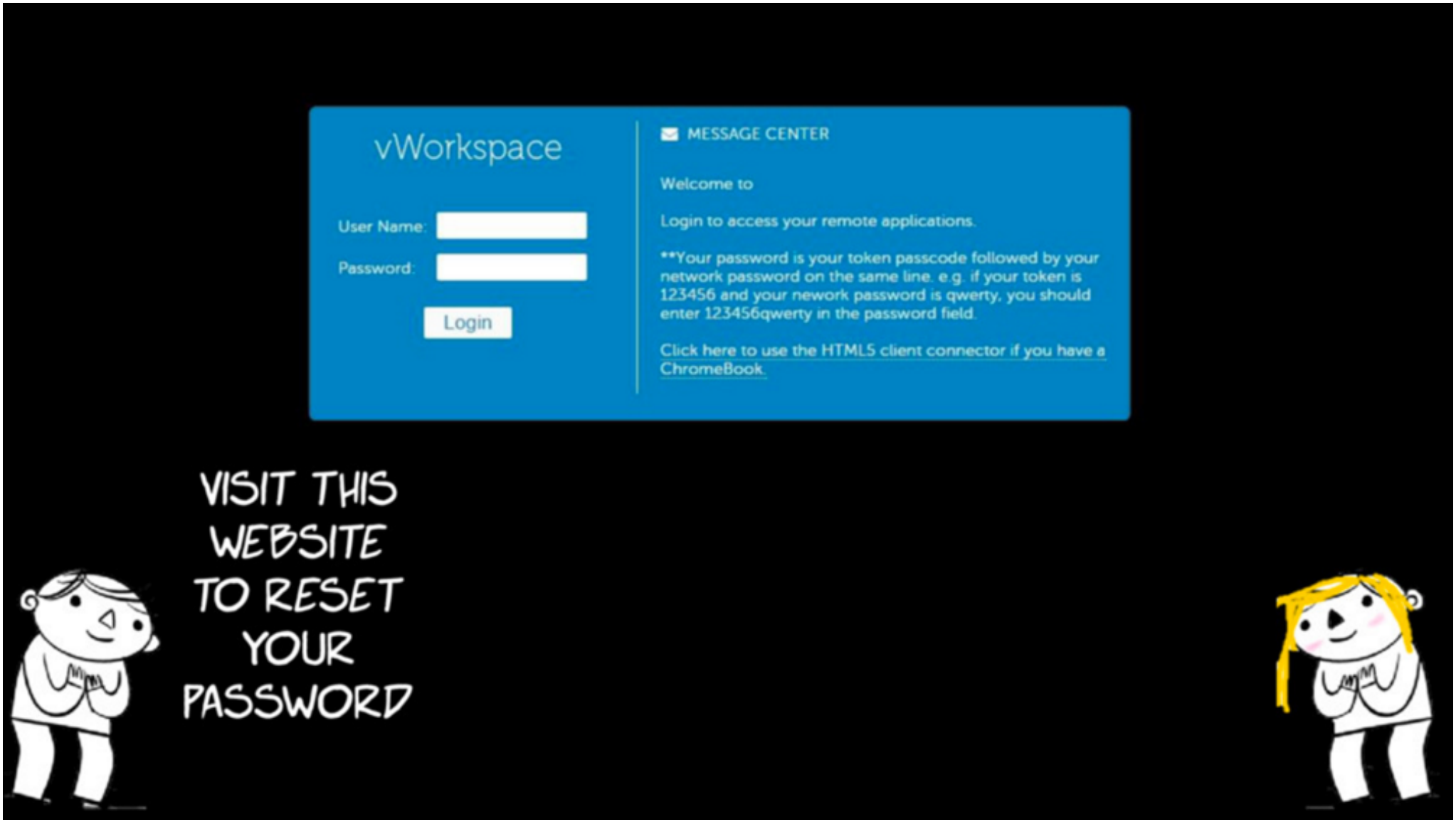
I FORGOT MY
PASSWORD



I FORGOT MY
PASSWORD
OH AND I
DON'T HAVE MY
LAPTOP
BECAUSE I'M
TRAVELLING

I FORGOT MY
PASSWORD
OH AND I
DON'T HAVE MY
LAPTOP
BECAUSE I'M
TRAVELLING
AND I REALLY
NEED ACCESS
TO MY
ACCOUNT
CAN YOU
PLZ HELP?

YA SURE


vWorkspace
User Name:
Password:
Login
MESSAGE CENTER
Welcome to
Login to access your remote applications.
**Your password is your token passcode followed by your network password on the same line. e.g. if your token is 123456 and your nework password is qwerty, you should enter 123456qwerty in the password field.
Click here to use the HTML5 client connector if you have a ChromeBook.
VISIT THIS WEBSITE TO RESET YOUR PASSWORD

REQUIRE

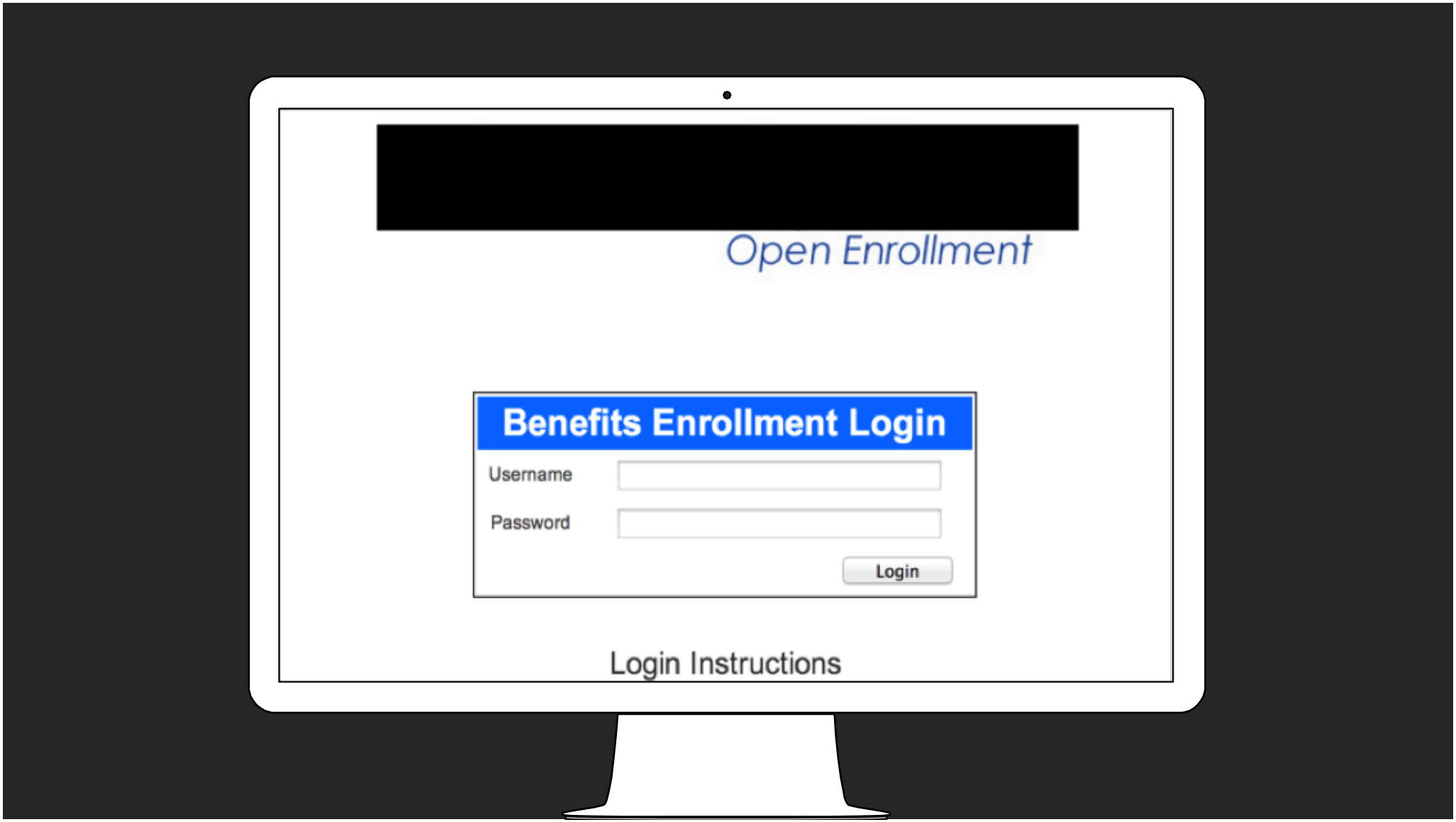
Verb

- Need for a particular purpose
- Cause to be necessary

Email Phishing

National Retail Company

- Impersonate the head of Human Resources
- Convince employees to log in to fake benefits portal
- Gain access to internal network and resources


[redacted]
Open Enrollment
Benefits Enrollment Login
Username
Password
Login
Login Instructions

Incident Response Failures

- Employees did not know who to report to
- IR team did not know who was affected
- No enforcement of IR policy
- Allowed for persistent access to the internal network

I followed the instructions and was not able to log in. Please advise

This is not a legitimate email from the Benefits Department. DO NOT DO ANYTHING!

Hackers gonna hack. Or, at least try to.

I followed the instructions and was not able to log in. Please advise

This is not a legitimate email from the Benefits Department. DO NOT DO ANYTHING!

Hackers gonna hack. Or, at least try to.

The following email was brought to the attention of information security. Please do not click the link or respond to it.

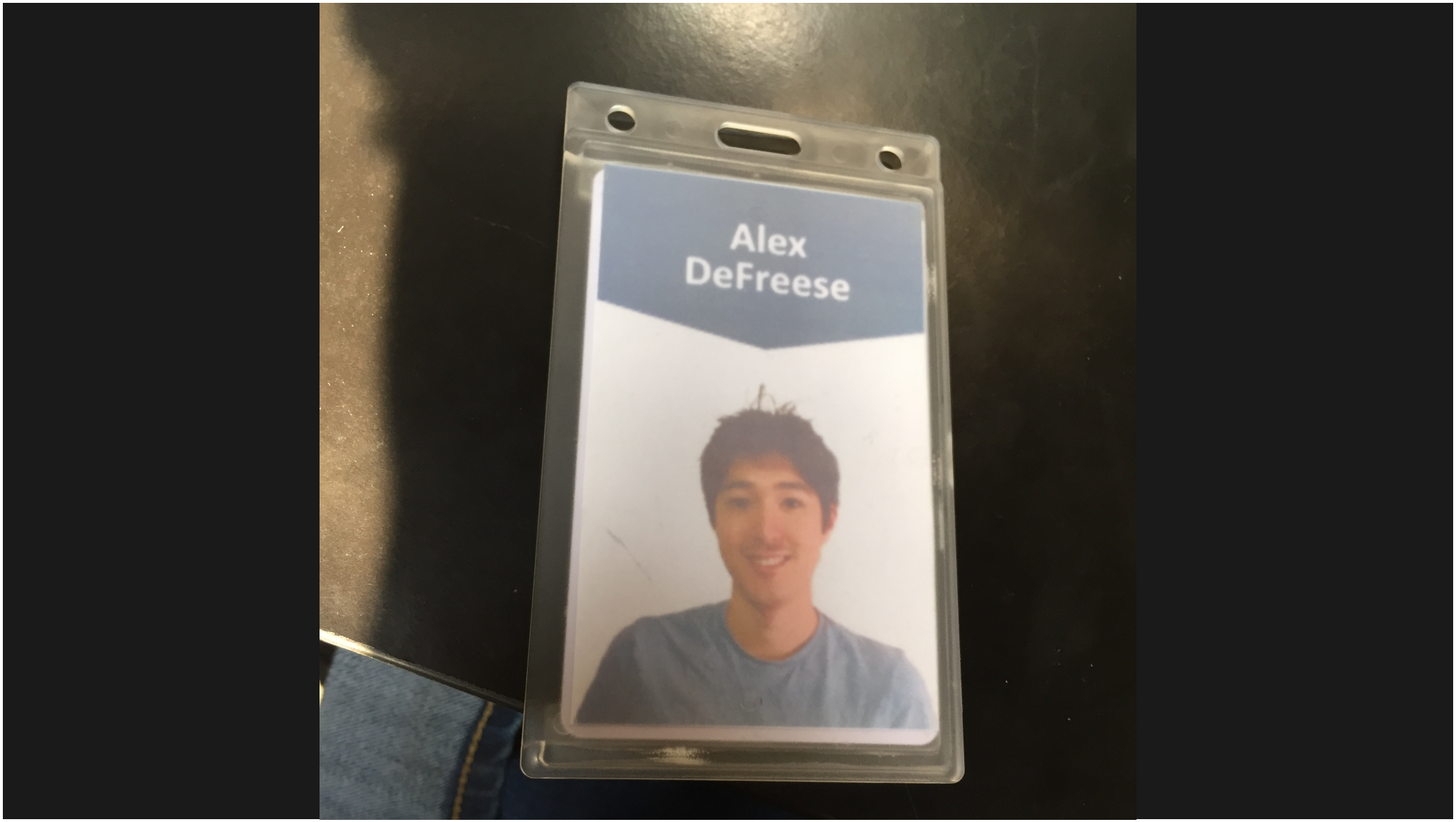
Questions? Contact infosecoperations@[redacted].com.

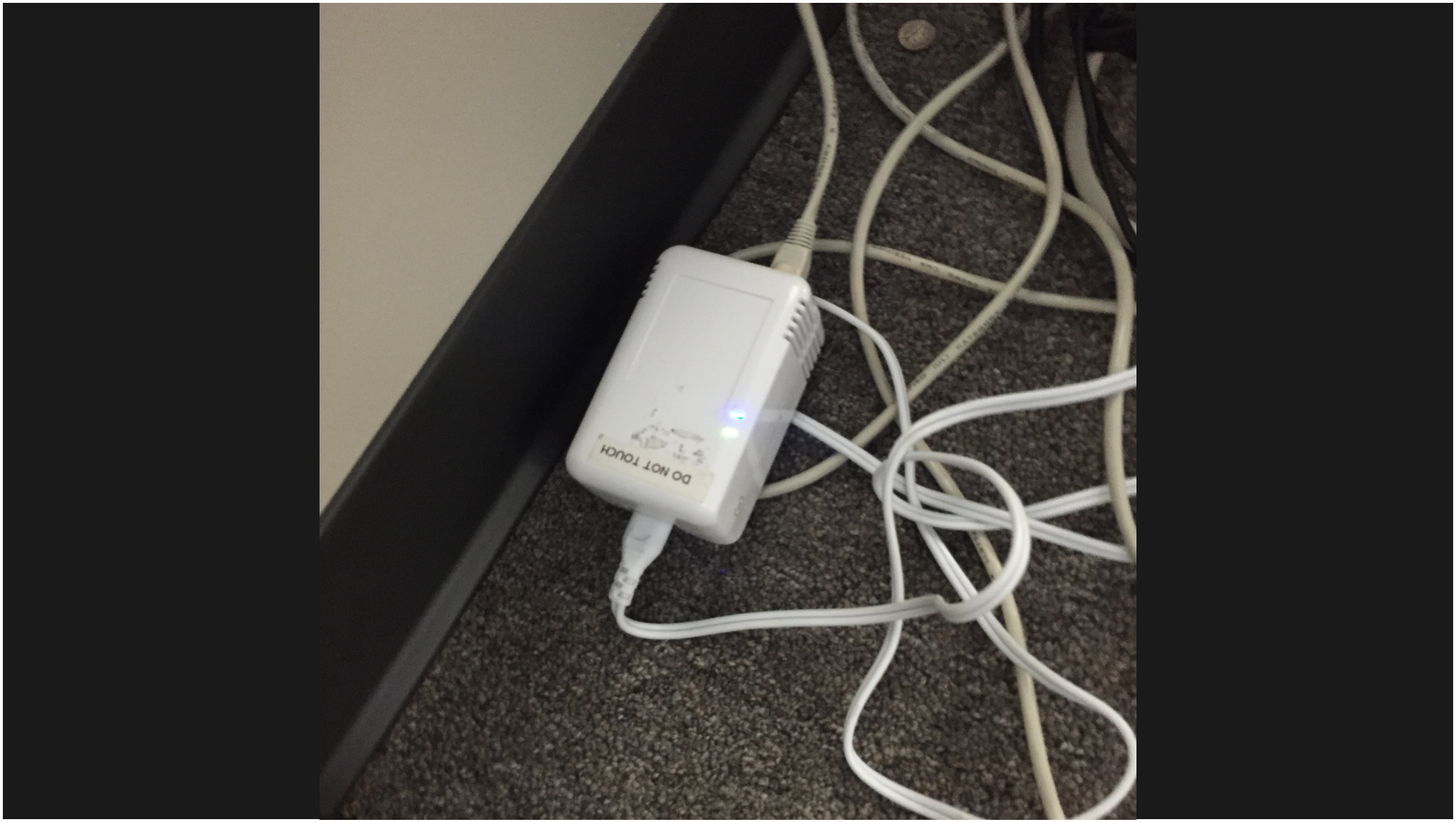
Quick Wins

Physical Access

National Banking Institution

- Impersonate IT contractors
- Gain access to network ports
- Plug in rogue device and gain access to internal network


Alex
DeFreese


DO NOT TOUCH

Quick Wins

Better

Improving the Incident Response

Phone Social Engineering

National Retail Company

- Impersonate an employee
- Call helpdesk for password reset
- Gain access to internal network and resources

Kirill Wright/Shutterstock

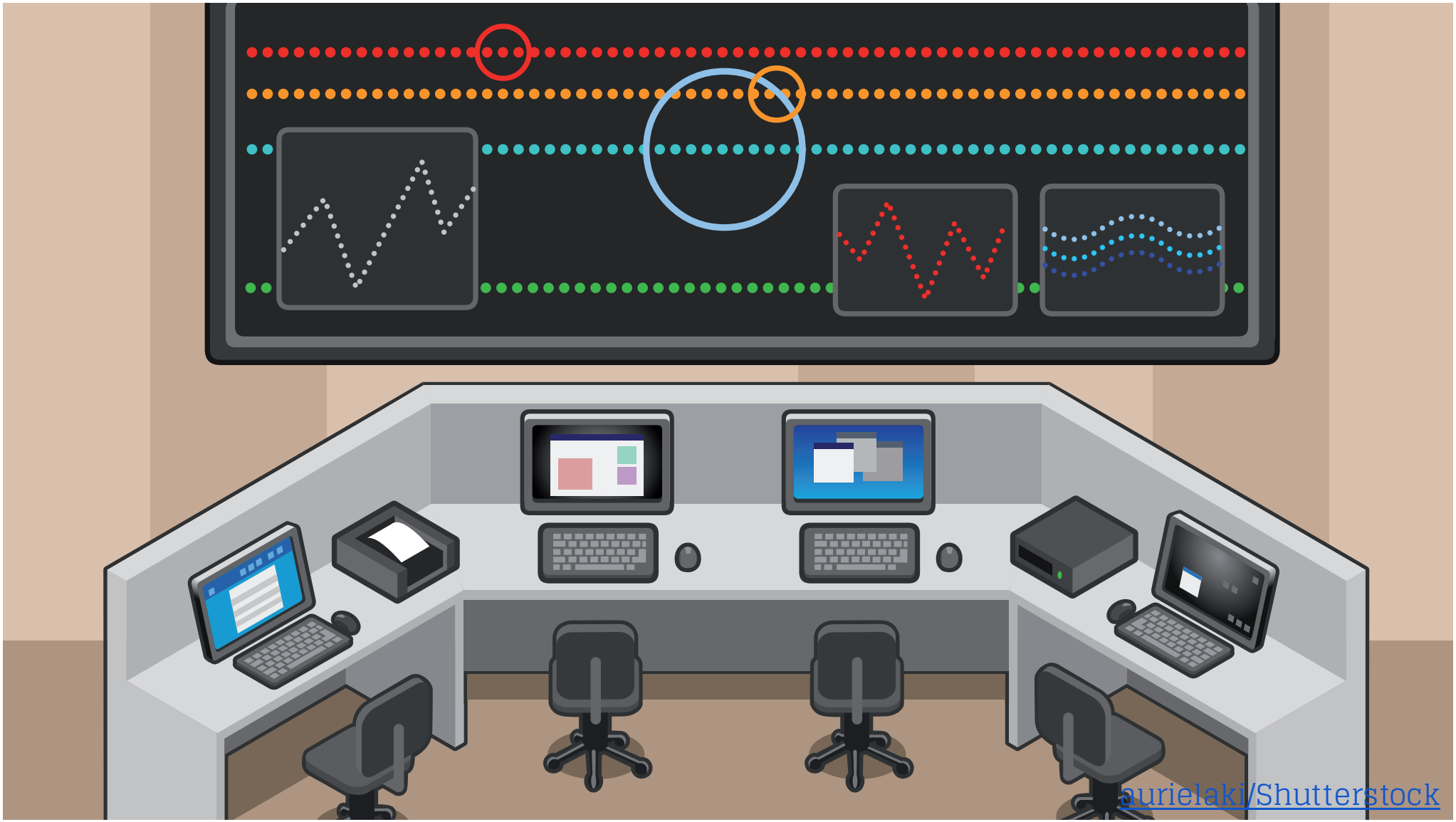
Quick Wins

Email Phishing

National Retail Company

- Impersonate automated emails
- Convince employees to log in to fake OWA pages
- Gain access to internal network and resources

wk1003mike/Shutterstock



aurielaki/Shutterstock

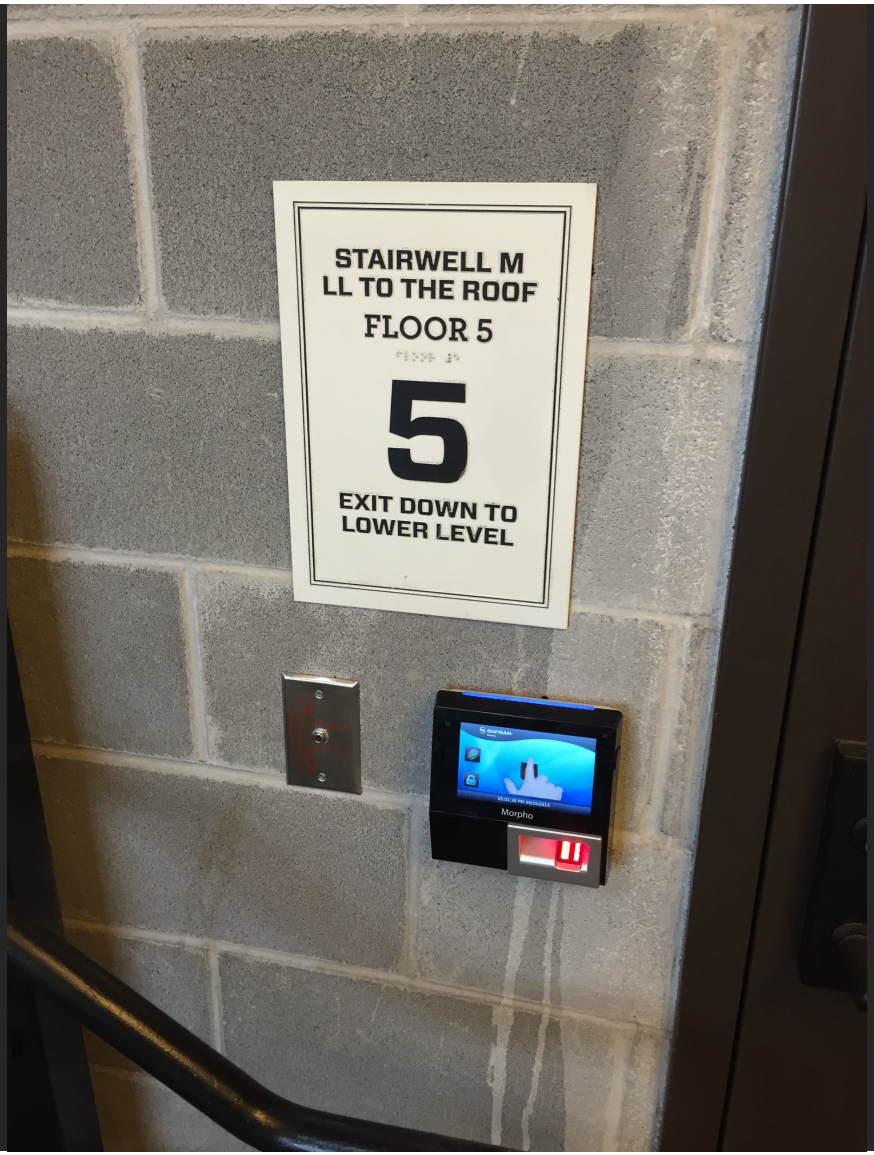
Quick Wins

Physical Access

Email Marketing Company

- Bypass fingerprint reader to gain access to office
- Use USB device to gain code execution on a laptop
- Gain access to internal network and resources


5


STAIRWELL M
LL TO THE ROOF
FLOOR 5
5
EXIT DOWN TO
LOWER LEVEL
Morpho


ATMEL
32UC3A1
256-U
0818 758-4

Quick Wins


Best

Do you know what to do?

Does anyone else?

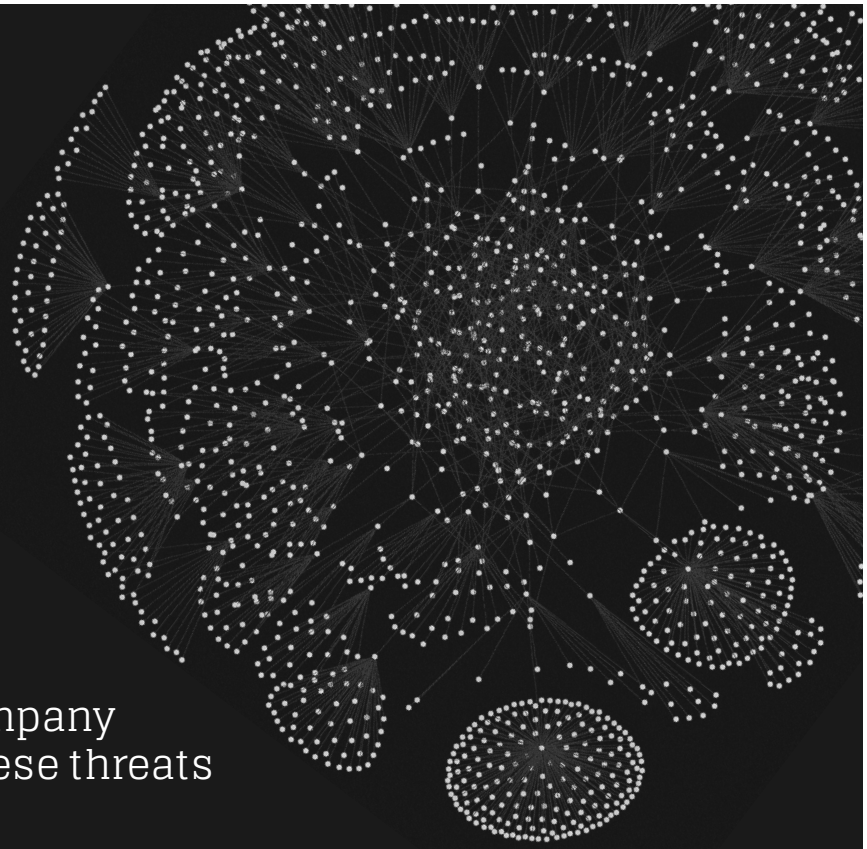
What happens when...

Employees start receiving large scale phishing emails?

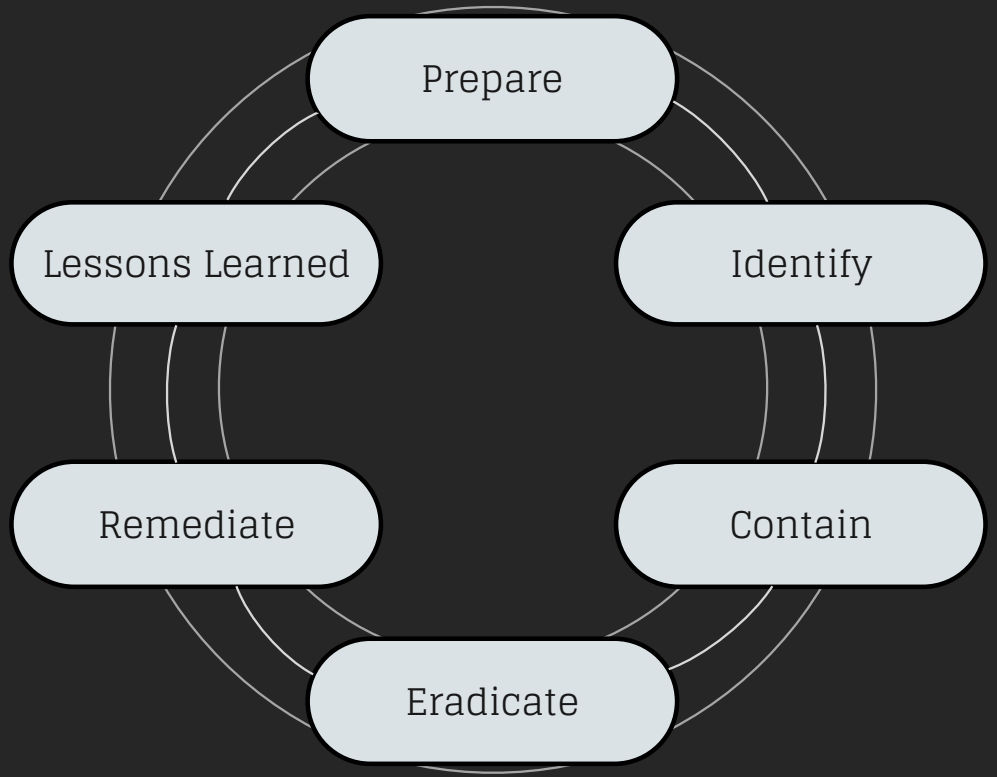
All network shares are suddenly encrypted?

Malware is detected running on a computer?

TAILORED INCIDENT RESPONSE PLAN



- Identify the most common threats facing your company
- Define and enforce incident response plans for these threats



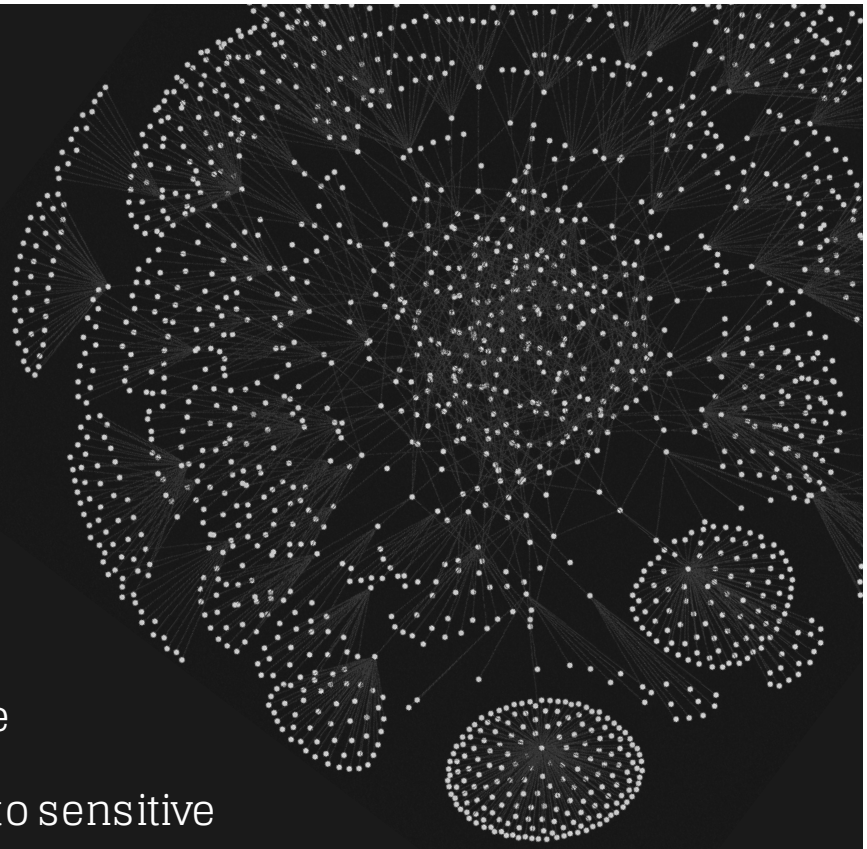
INCIDENT RESPONSE LIFECYCLE

https://cert.societegenerale.com/en/publications.html


Tactical Recommendations

Phone Social Engineering

AUTHENTICATION FOR SENSITIVE ACTIONS

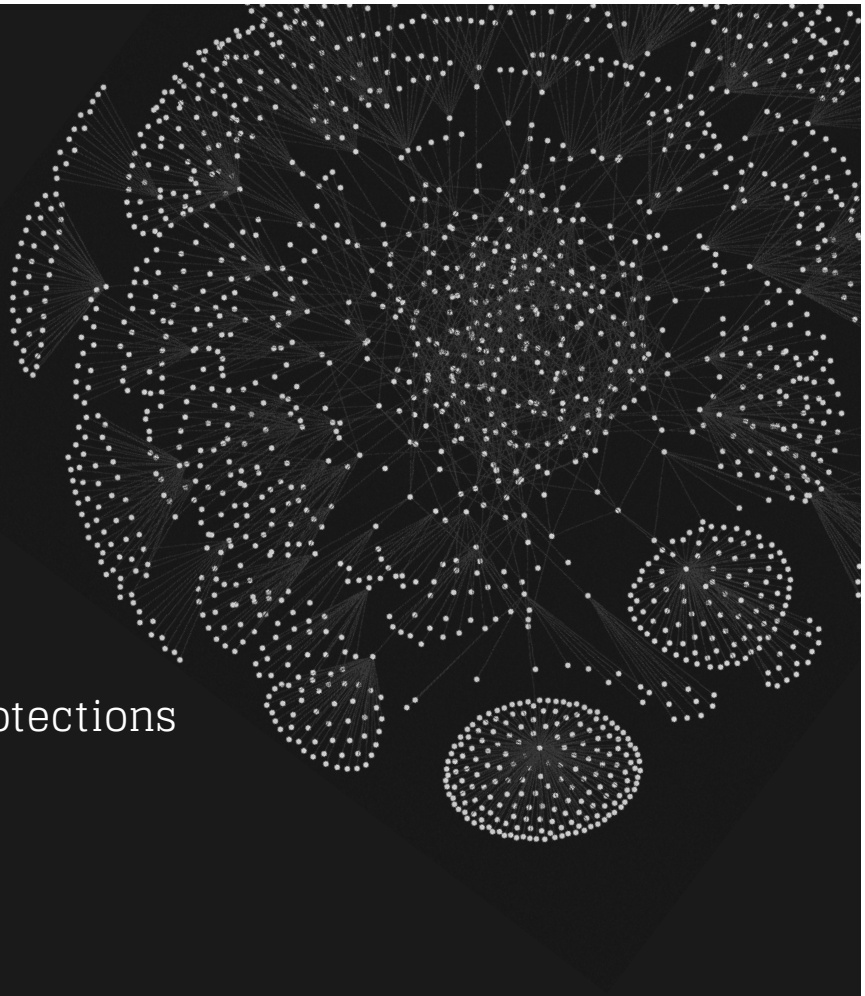


- Require authentication before accessing sensitive information
- Focus training on employees who require access to sensitive information
- Remove access to sensitive information for those that don't need it

Email Phishing


Email Protections

LIMIT ATTACKER OPTIONS

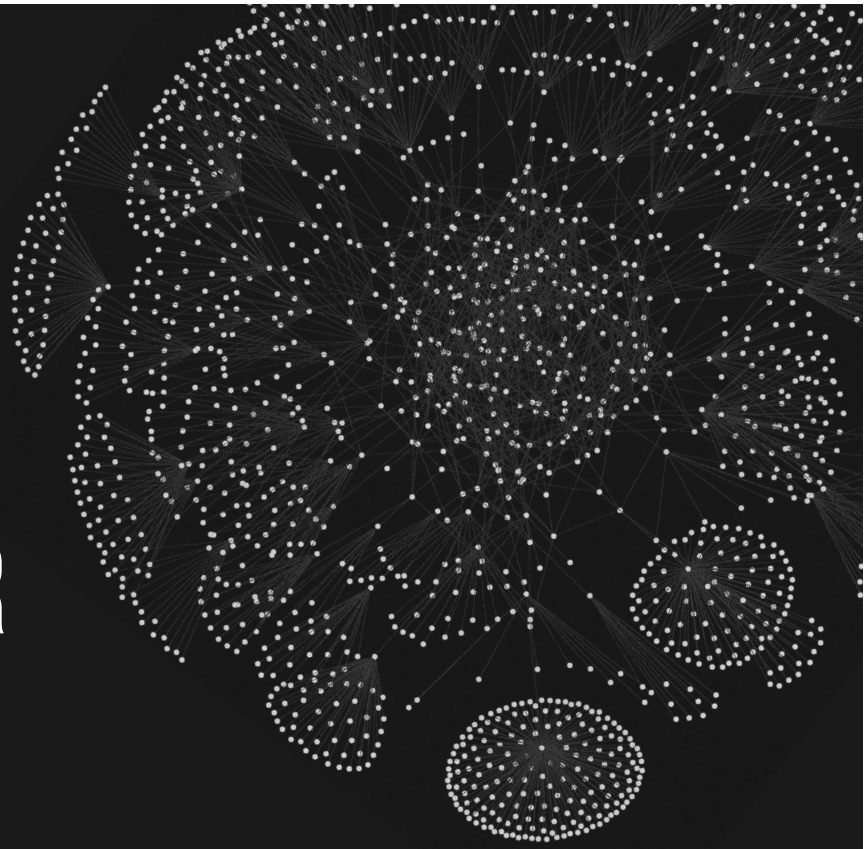


- Prevent email spoofing by implementing email protections
- Monitor or buy domains similar to your own
- Heuristic phishing detection
- Identification of email recipients

Physical Access

monticello/Shutterstock

UNDERSTAND THE PERIMETER

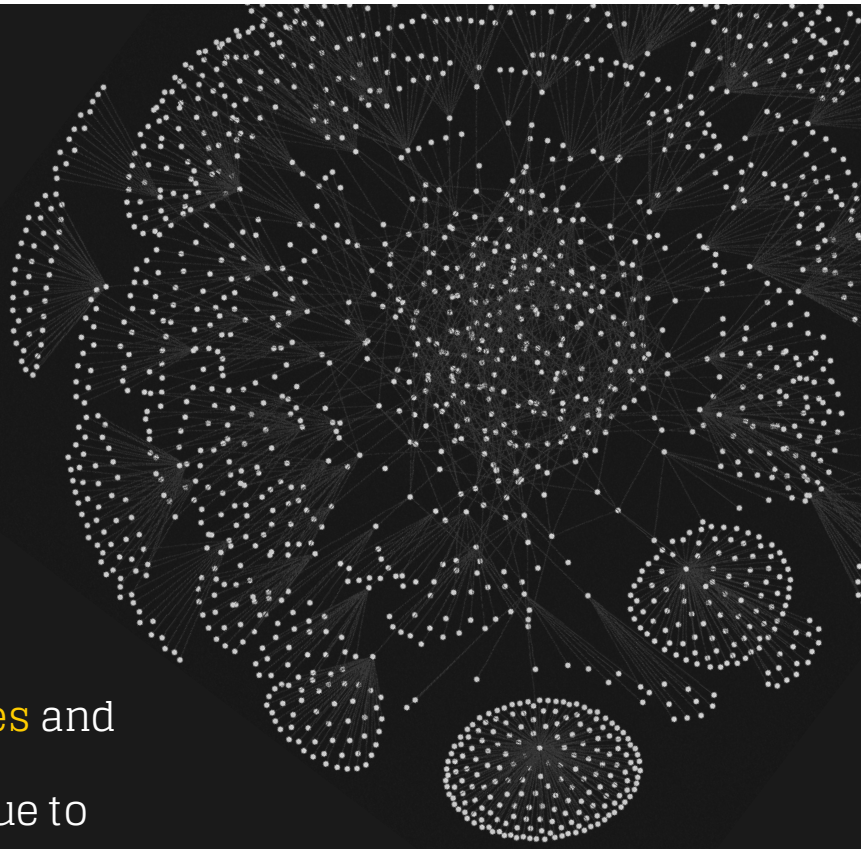


- Turnstiles and guards for ingress points
- Network access controls
- Badges and escorts for guests
- Screen lock policy
- Host-based and network detection capabilities

Strategic Recommendations

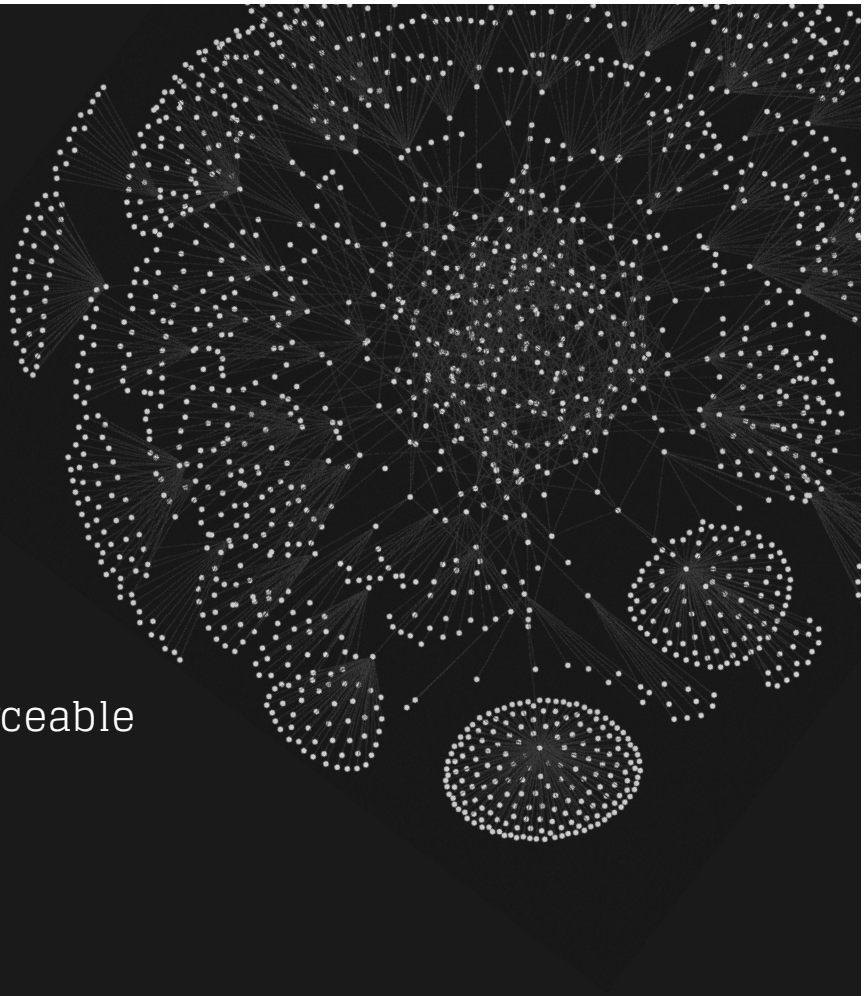
POLICY, PROCESSES, PEOPLE

- Technical controls provide enforcement for policies and processes
- Without enforcement, social engineers will continue to exploit the people



ENFORCE PROCESSES

- When performing sensitive actions, focus on enforceable processes
- Authentication enforces who they are
- Authorization enforces what they're allowed to do



Conclusions

1. Every organization will be compromised by human error

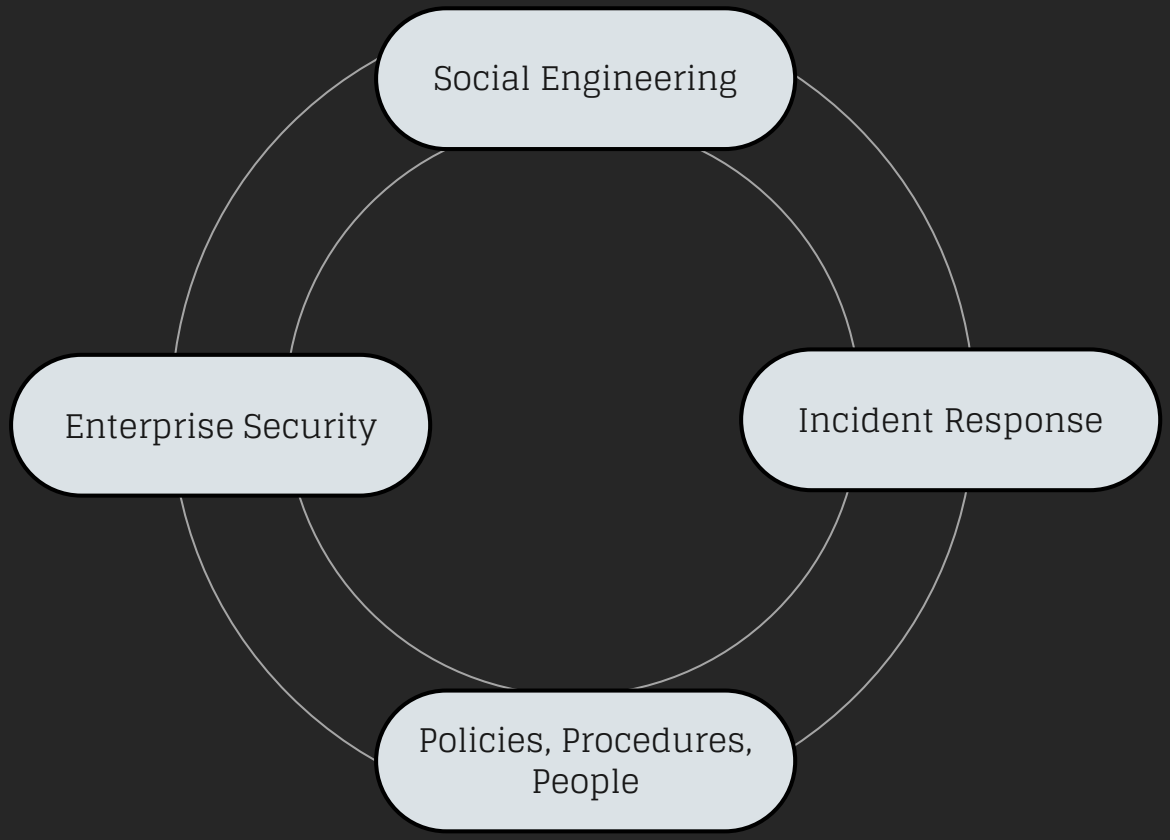
1. Every organization will be compromised by human error

2. Require policies and processes be enforced

1. Every organization will be compromised by human error

2. Require policies and processes be enforced

3. Continued assessment improves risk mitigation



RINSE AND REPEAT

Thanks!

Any questions ?

You can find us at:

- @bishopfox
- facebook.com/bishopfoxconsulting
- linkedin.com/company/bishop-fox
- google.com/+bishopfox

CREDITS

Christina Camilleri (@0xkitty) for the slide design!