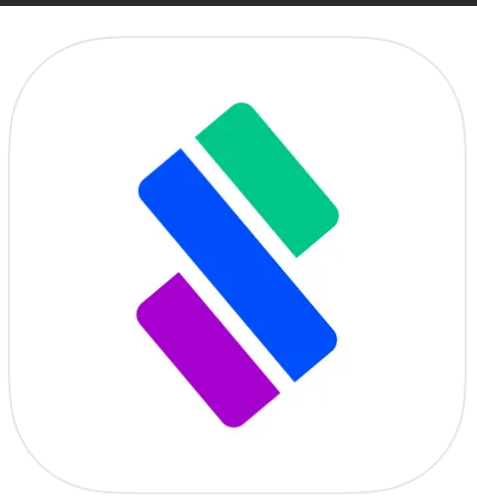
SO, HAVE YOU HAD A SECURITY CONVERSATION YET?



Cyware Social 17+

Cyber Security & Hacker News

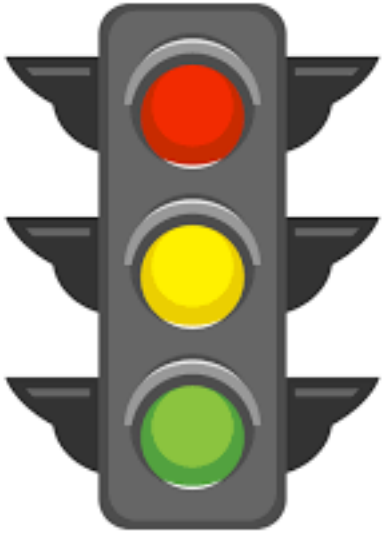
Cyware Labs Inc

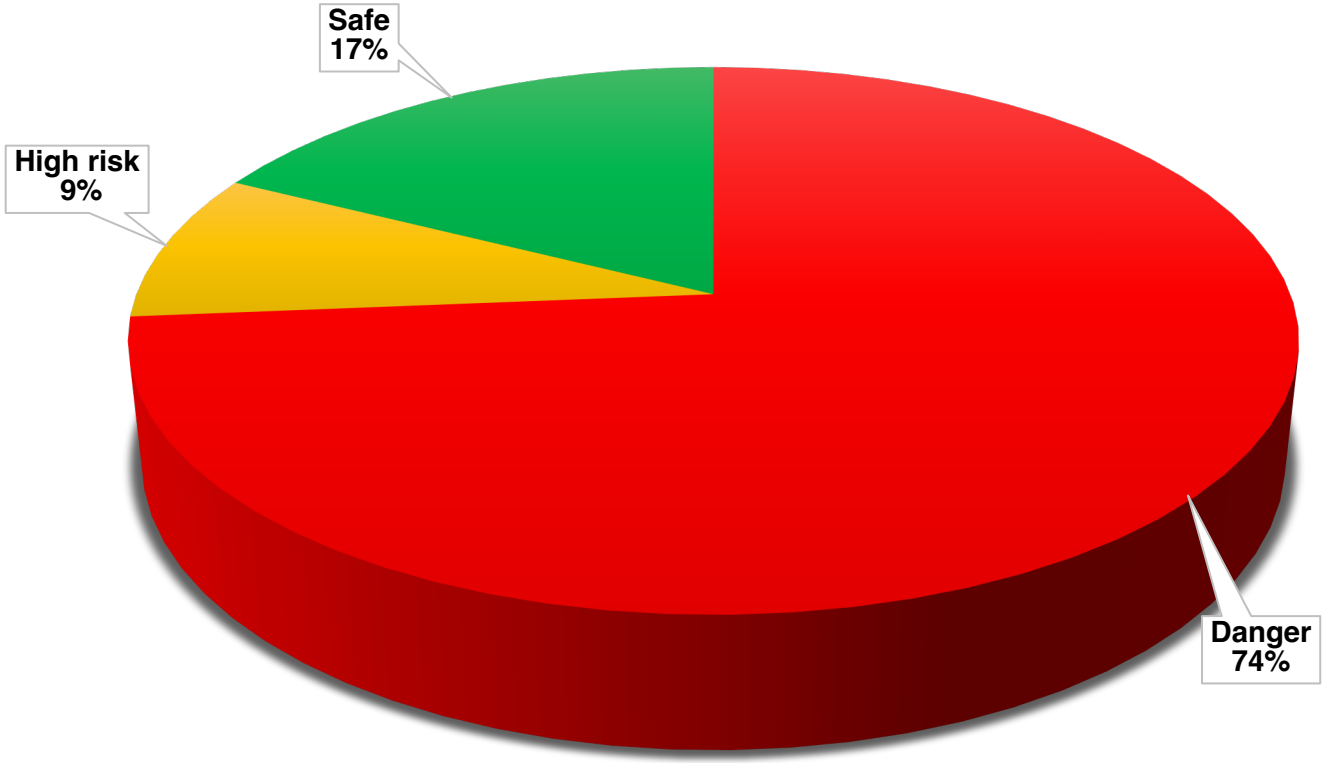
★★★★½ 4.6 • 38 Ratings

Free

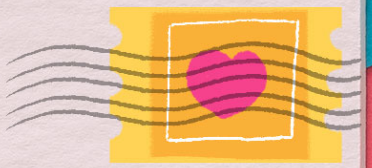
THE INTERNET HAS SOME DESIGN FLAWS

SAMPLE OF TNP CUSTOMERS

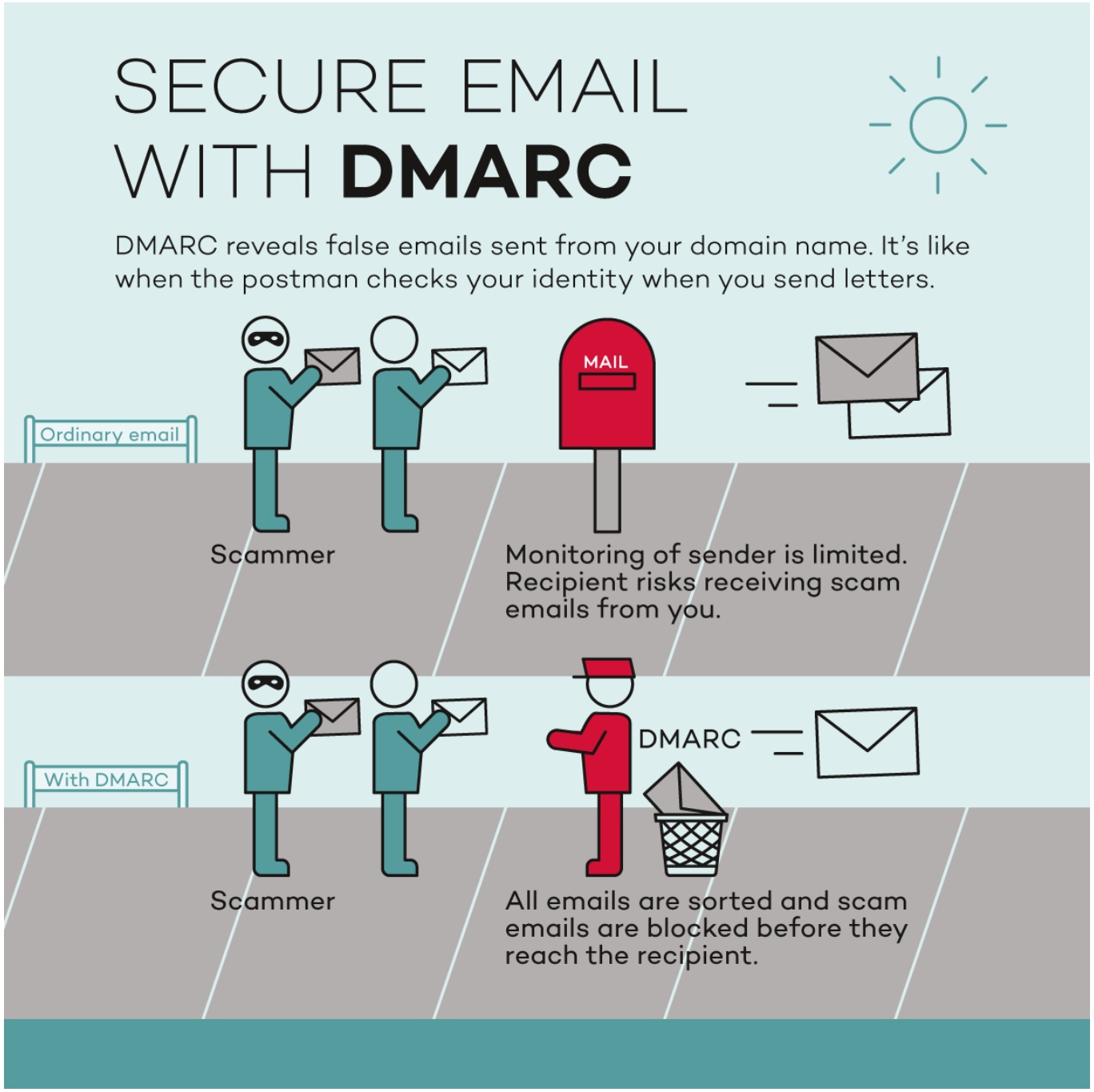




MS. JANE H. DOE
40 THEATRE STREET
SUN CITY, AZ 85351
USA



HR. GUÐMUNDUR ÁRNASSON
TRYGGVAGÖTU 5
220 HAFNARFIRÐI
ICELAND



HOW DMARC WORKS

DMARC IS THE SOLUTION FOR EMAIL VERIFICATION

- Without DMARC I can send an email **pretending to be your CEO without hacking into your email system**
- This is a great way to phish your customers and destroy **your reputation**
- **Turning on DMARC signals to hackers that you have an improved cyber posture**
- **Hackers can see your DMARC status, so can we.**

94% OF **PHYSICAL** HOSTAGE SITUATIONS THE CRIMINAL LOSES

60% OF RANSOMWARE SITUATIONS ARE UNSUCCESFUL

80% OF RANSOMWARE STARTS WITH A PHISHING ATTACK

TARGETED FOR 100 DAYS AVERAGE


Accident

MAERSK

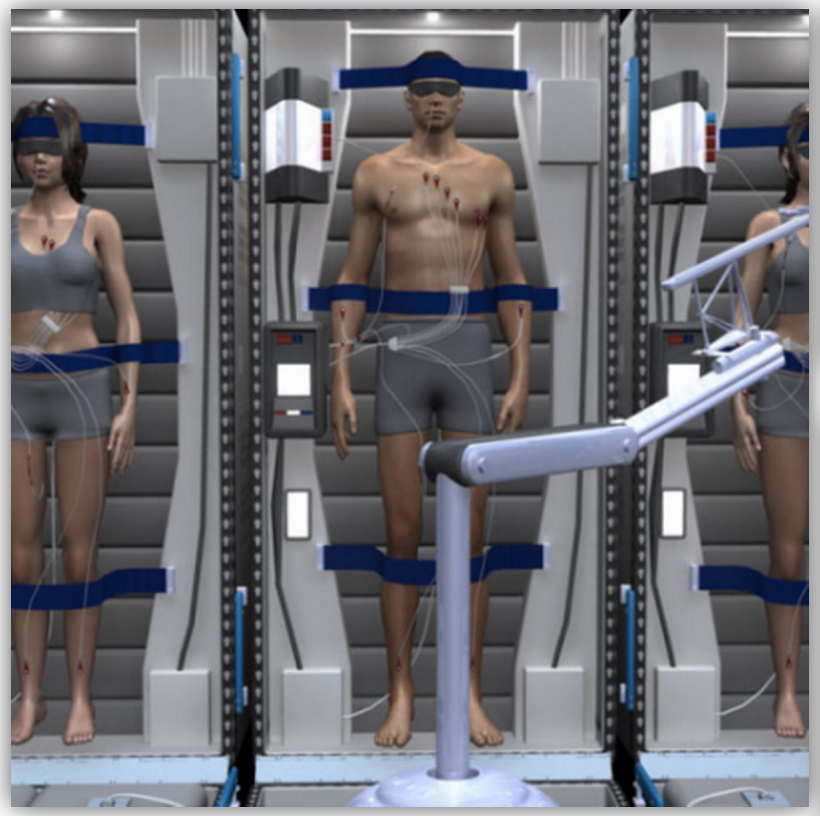
- Lost $300m in lost business
- $10m in restoration costs
- $0 ransom, and WERE NEVER TARGETED

UKRAINE

Tech › Tech news

NO DELIVERY YODEL HACKED: Millions of customers face parcel delays after delivery service hit by cyber attack

Royal Mail



SOLUTIONS?

PREPARE

DEFEND

RESPOND

IMMUTABLE STORAGE

MULTIPLE BACKUPS

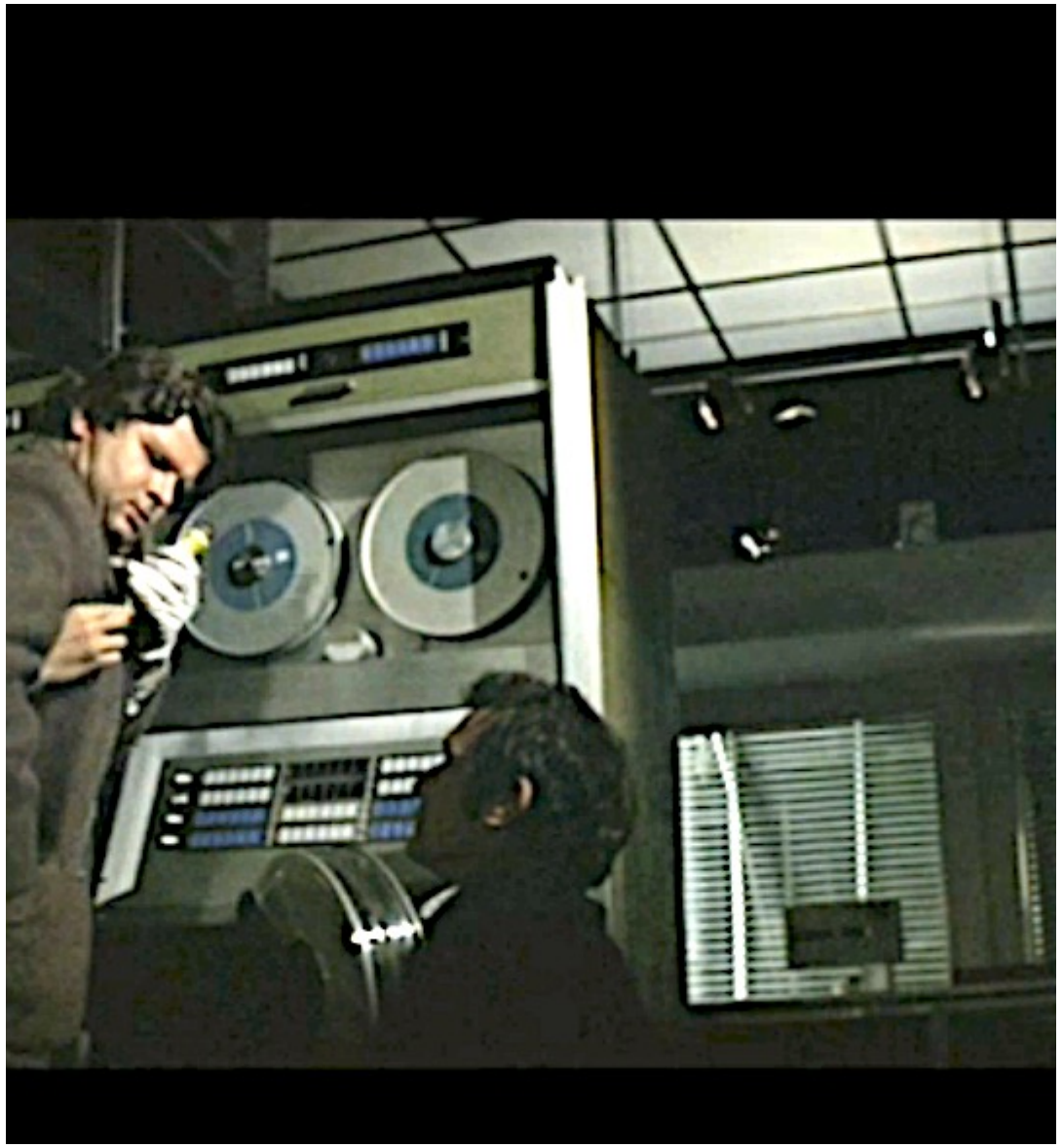
GOOD DEFENCES

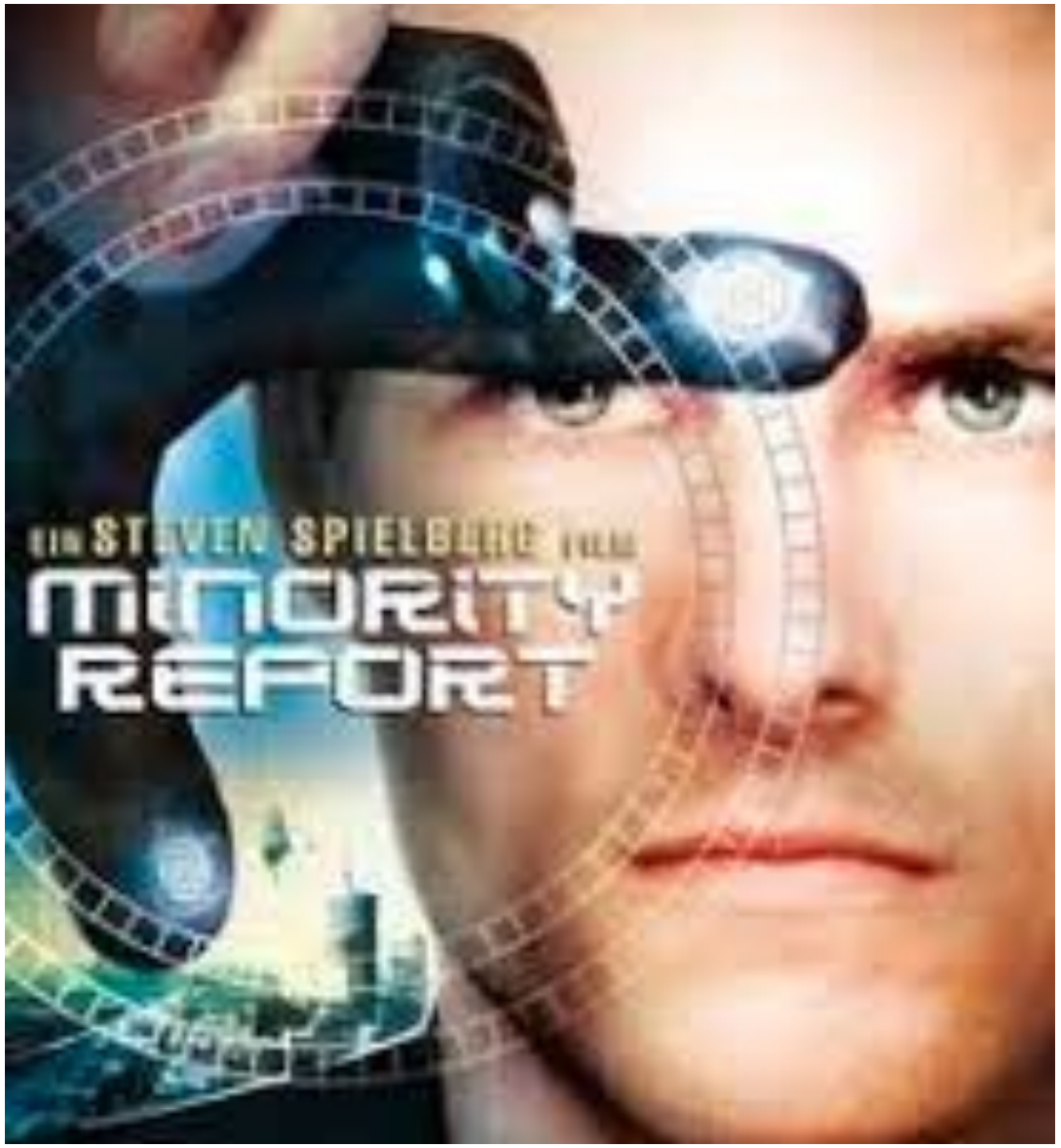
TAKE DOWN AND SOC SERVICES

DARK WEB SCANNING

DARK WEB NEGOTIATORS

EXEC CRISIS SIMULATION




A STEVEN SPIELBERG FILM
MINORITY
REPORT


"PRE-CRIME" FEEDS
ARE NOW AVAILABLE

UK UNIVERSITY RANSOMWARE ATTACK

OPPORTUNITY

12 months prior to attack

>3,100 student and staff emails and passwords appeared on leak sites

HOSTILE INTENT

>1 month prior to attack

Chatter about the University on dark web forums and listings increases

CAPABILITY

>1 month prior to attack

Communication between Tor nodes and compromised email addresses (to test validity of these addresses)

RANSOMWARE

On the day of the attack

University suffers a ransomware attack. Its internal network is down & campus closed to all 25K students for 12 days

WITH SEARCHLIGHT, THE UNIVERSITY COULD HAVE PRE-EMPTED AND PREVENTED THIS COSTLY ATTACK

SEARCHLIGHT

TRADITIONAL SOC SERVICES

1

RECONNAISSANCE

HARVESTING EMPLOYEE EMAILS ADDRESSES AND CREDENTIALS, PROBING THE NETWORK IN SEARCH OF VULNERABILITIES.

2

WEAPONIZATION

COUPLING THE EXPLOIT WITH A BACKDOOR TO CREATE A DELIVERABLE PAYLOAD.

3

DELIVERY

DELIVERING THE WEAPONIZED BUNDLE TO THE VICTIM, FOR EXAMPLE THROUGH EMAIL, WEB, USB OR CLOUD APPLICATION.

4

EXPLOITATION

EXPLOITING A VULNERABILITY TO EXECUTE CODE ON THE VICTIM'S SYSTEM.

5

INSTALLATION

INSTALLING MALWARE ON THE ASSET.

6

COMMAND AND CONTROL (C2)

ESTABLISHED A COMMAND CHANNEL TO AN EXTERNAL SERVER FOR REMOTE MANIPULATION OF THE VICTIM.

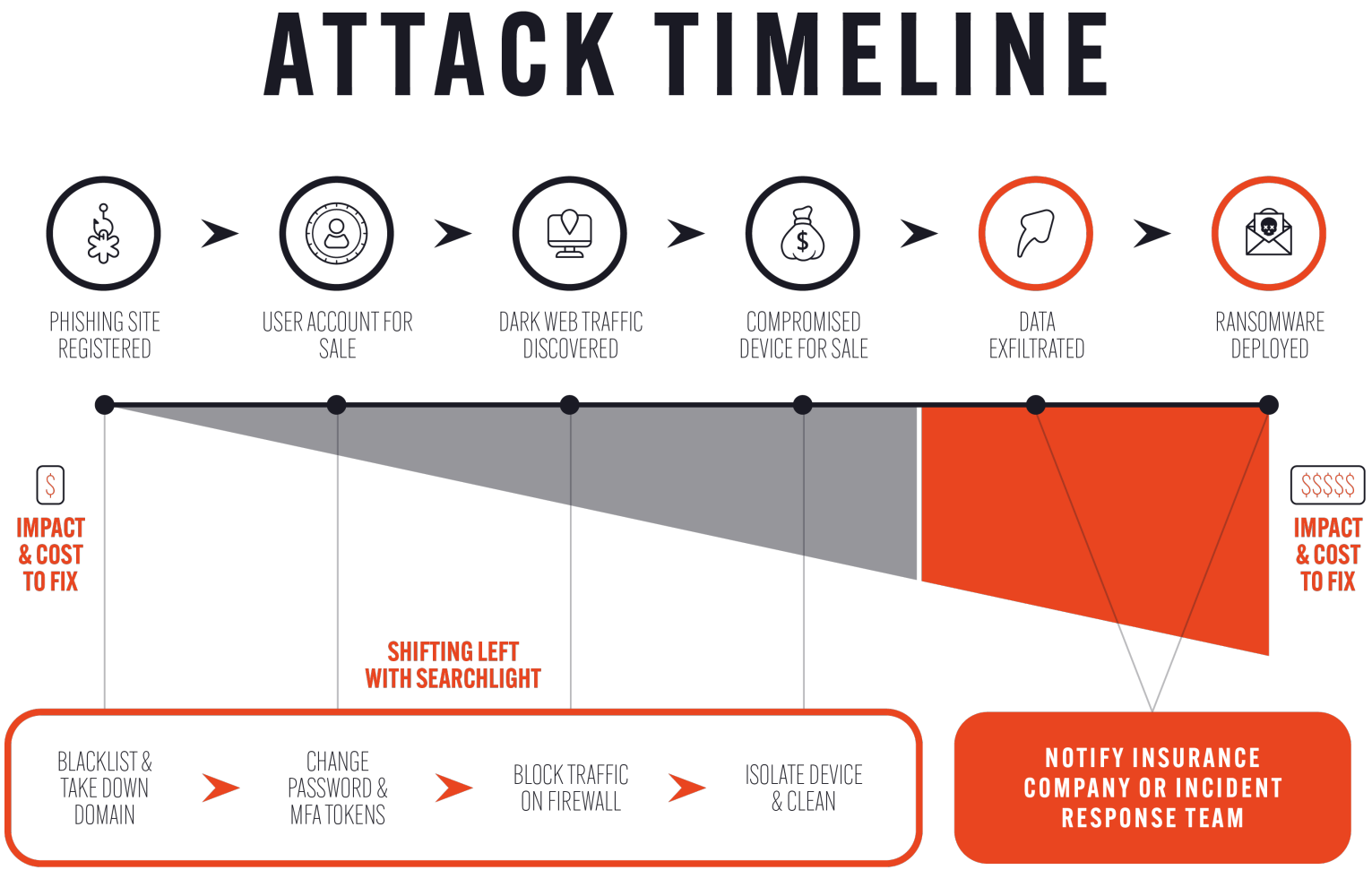
7

ACTIONS ON OBJECTIVES

FOR EXAMPLE, DATA EXFILTRATION, RANSOMWARE DEPLOYMENT OR CORPORATE ESPIONAGE.

SHIFT LEFT IN THE CYBER KILL CHAIN

Take decisive action before an attack



THE VALUE OF EARLY THREAT INTELLIGENCE

Identify the early indicators of an attack to defend your people and revenue


WHALING
FOR
BEGINNERS
Jerome Vincent

IMMUTABLE STORAGE: NAV VAULT