

Part 1: Healthcare Cyber Threat Landscape

proofpoint

Mike Yriart

Senior Account Manager – HealthCare



Intro: Mike Yriart

- Senior Account Manager, HealthCare

Past Professional Roles: IT Strategy, Process Engineering
and Project Management















Happy Husband - Proud Dad
Into Outdoor Adventure



proofpoint.

Largest Healthcare Breaches of 2022

 <p>Patients Impacted: 4.11M Breach Method: Ransomware</p>	 <p>Patients Impacted: 3.0M Breach Method: EMR Access</p>	 <p>Patients Impacted: 2.21M Breach Method: Hacking</p>	 <p>Patients Impacted: 2.0M Breach Method: Hacking</p>
 <p>Patients Impacted: 1.91M Breach Method: Ransomware</p>	 <p>Patients Impacted: 1.6M Breach Method: Malware</p>	 <p>Patients Impacted: 1.5M Breach Method: EMR Access</p>	 <p>Patients Impacted: 1.36M Breach Method: EMR Access</p>
 <p>Patients Impacted: 1.35M Breach Method: Hacking</p>	 <p>Patients Impacted: 1.29M Breach Method: Hacking</p>	 <p>Patients Impacted: 1.19M Breach Method: Ransomware</p>	 <p>Patients Impacted: 942K Breach Method: Ransomware</p>

Source: US Department of Health and Human Services Office for Civil Rights Breach Portal:
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Impacting Patient Safety...

The New York Times

Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack

A wave of damaging attacks on hospitals upended the lives of patients with cancer and other ailments. "I have no idea what to do," one said.



Colleen Cargill
Nurse, Oncology

"To look someone in the eye, and tell them they cannot have their life-extending or lifesaving treatment, it was horrible, and totally heart-wrenching," she said.

The very first person she turned away, a young woman, burst into tears. "She said, 'I have to get chemo, I am the mother of two young kids,'"

Ms. Cargill said. "She was so fearful, and the fear was tangible."



...and Costing Immensely...



HEALTH
ITSECURITY
xtelligent HEALTHCARE MEDIA

CommonSpirit Health Ransomware Attack Leads to \$150M in Losses To Date

As previously reported, CommonSpirit Health suffered a ransomware attack in October 2022 that impacted facilities across its network.



Universal Health Services Ransomware Attack Cost \$67 Million in 2020

Posted By HIPAA Journal on Mar 24, 2021

Why are Cyber Attacks on Healthcare Happening?

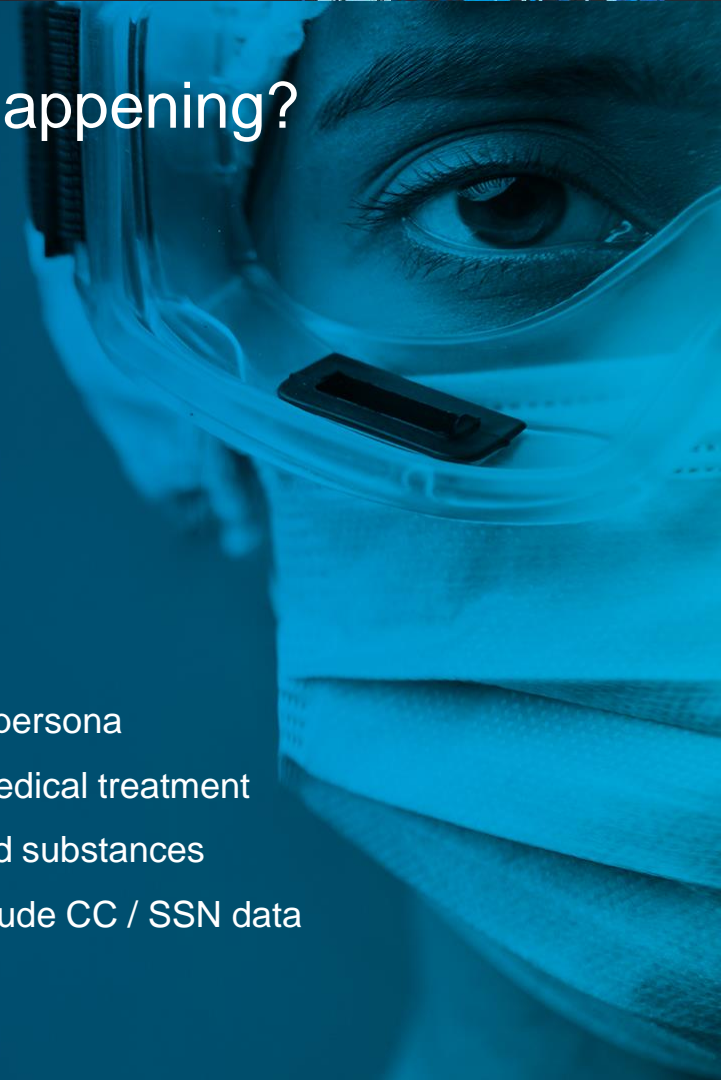
Healthcare Data is Highly Valuable

50x

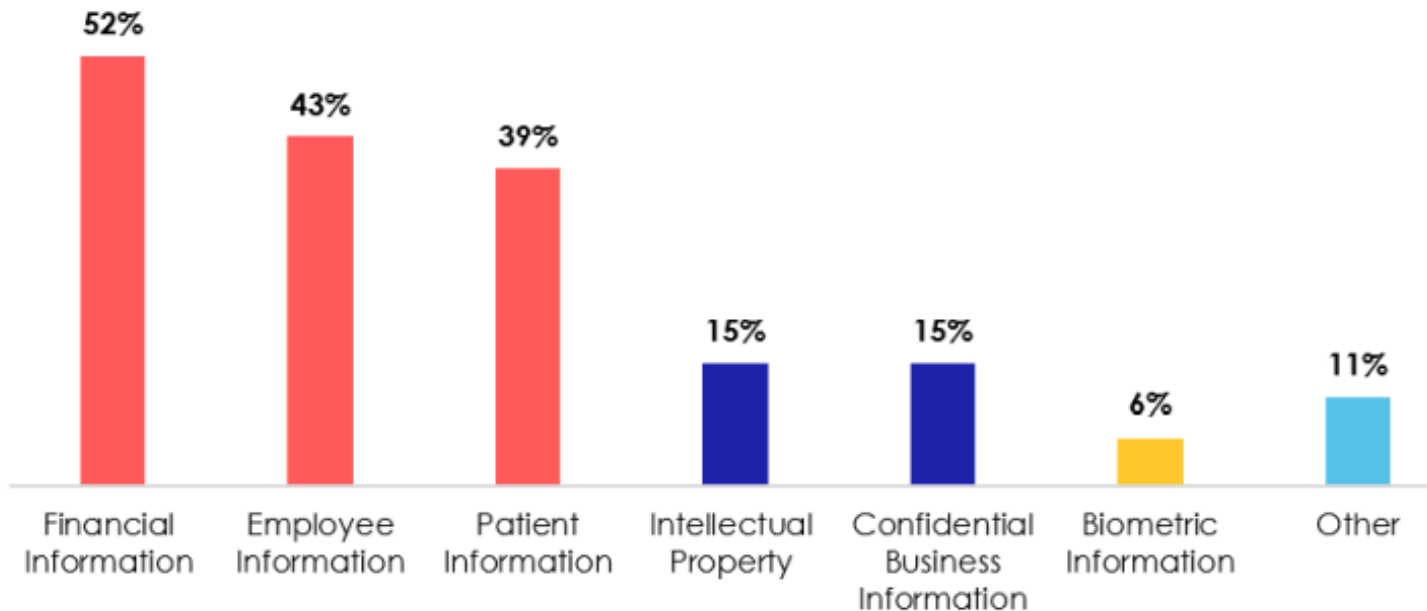
More valuable than credit card data

<https://www.dmagazine.com/healthcare-business/2019/10/why-medical-data-is-50-times-more-valuable-than-a-credit-card/>

- Create a whole persona
- Create / seek medical treatment
- Obtain controlled substances
- Many cases include CC / SSN data
- Long lifecycle

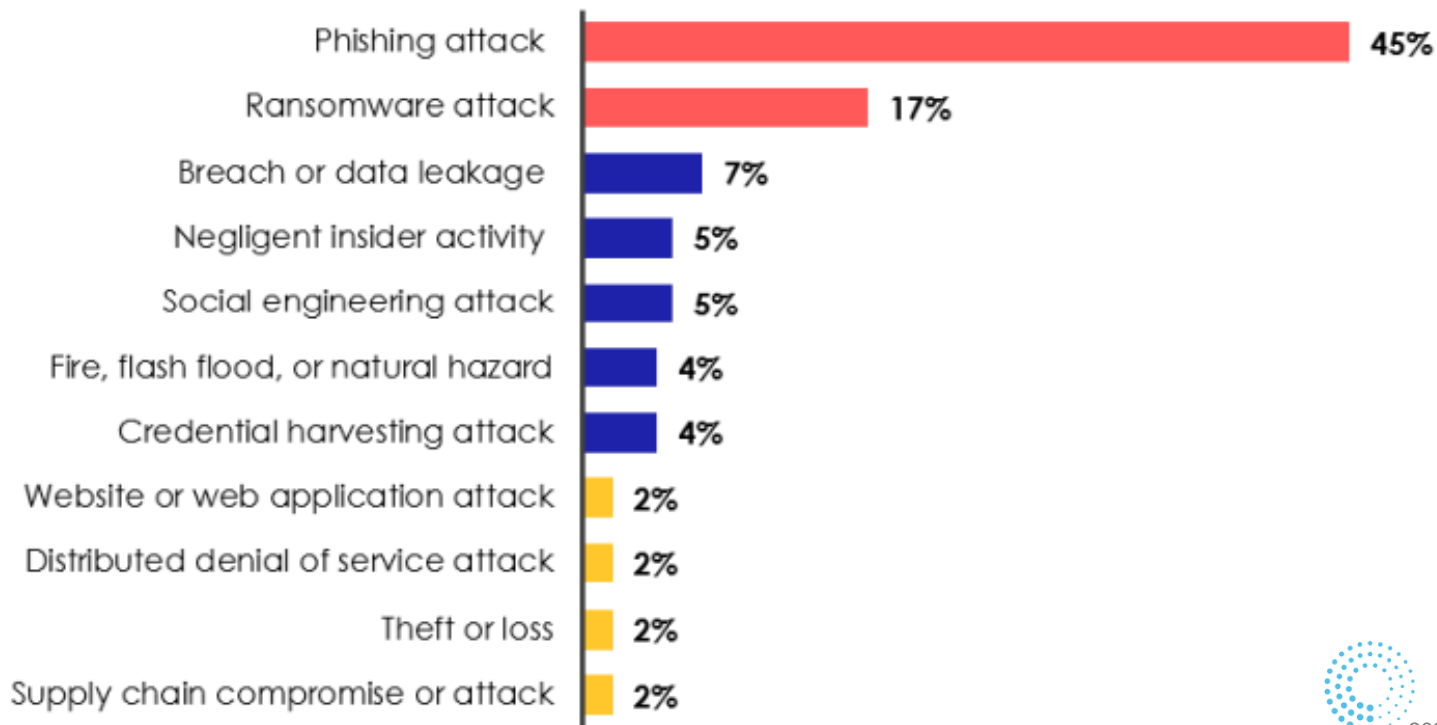


Threat Actor / Criminal Motivation...



How are Cyber-Attacks on Healthcare Happening?

People (Over Machines) Are Leveraged in Most Attacks



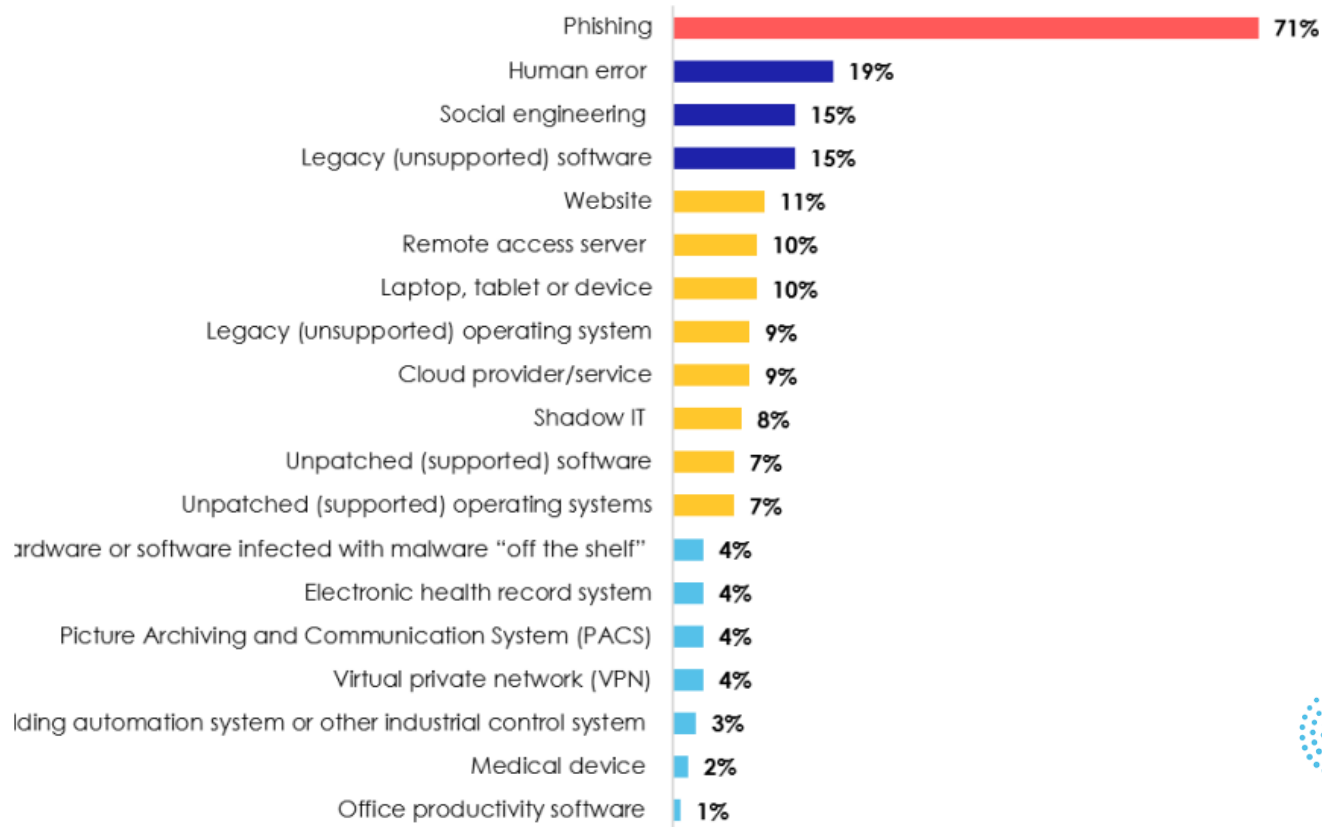
2021 HIMSS Healthcare Cybersecurity Survey

Finding:

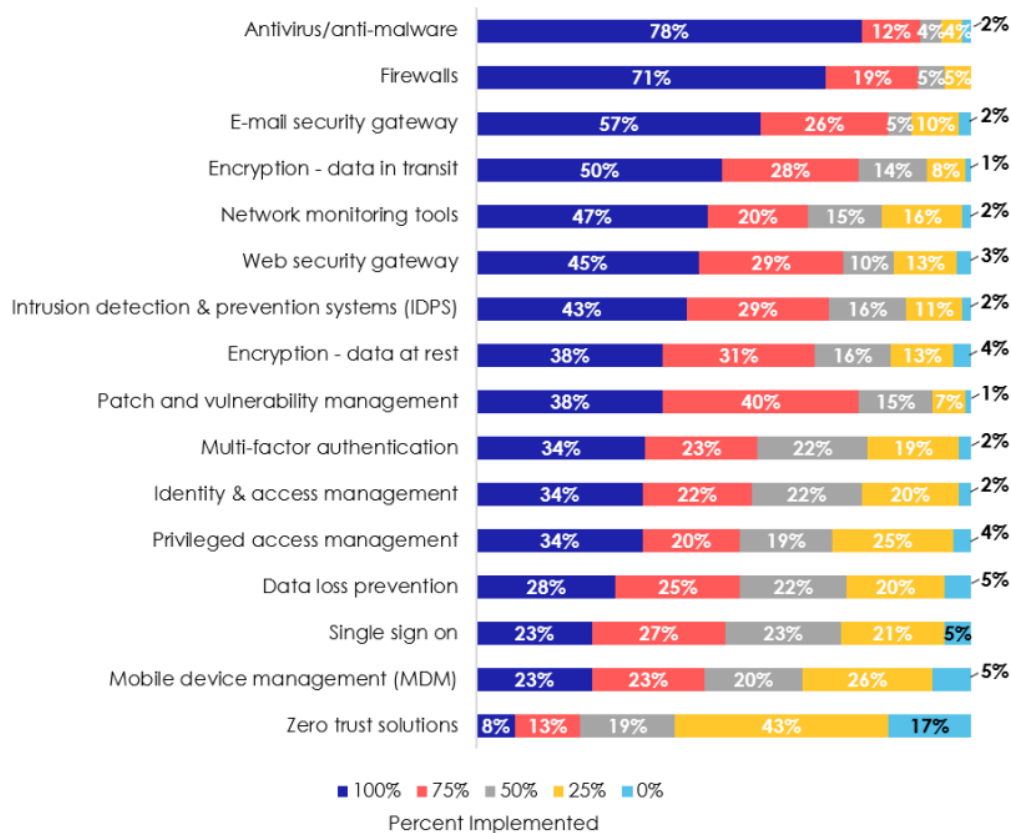
The Most Significant Security Incident:

- 🐟 **Phishing is still king.** Phishing leads the pack.
- 💰 **Financial information is the main target.** Threat actors typically go where the money is.
- 🖱️ **Initial hook is by phishing.** Phishing tends to be the initial point of compromise.
- 🔥 **Disruption is a typical impact.** Disruption is typical—whether organizations are prepared is another question.

The Initial Points of Compromise Ranked



Successful Attacks vs Level of Security



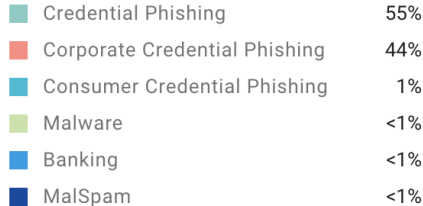
Modern Threat Landscape – What We See

1

Relentless focus on credential phishing

2020/09/23 - 2020/10/22

Sort by Attack Index Contribution

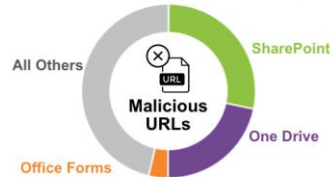


2

Legitimate filesharing abuse & attacks on O365

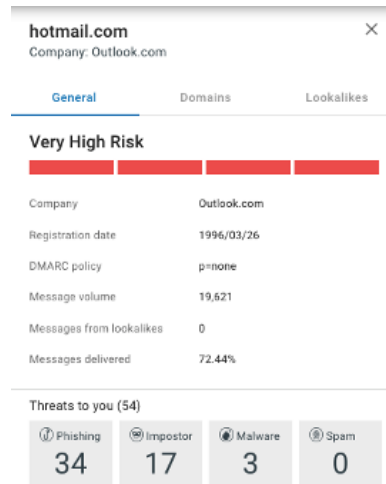
59,809,708+

Malicious messages targeted at Proofpoint customers sent or hosted by Microsoft Office 365 since December 2019



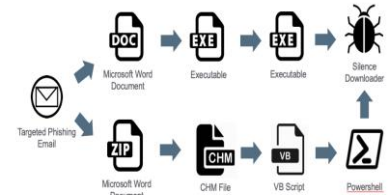
3

Business Email Compromise and Supply Chain variants

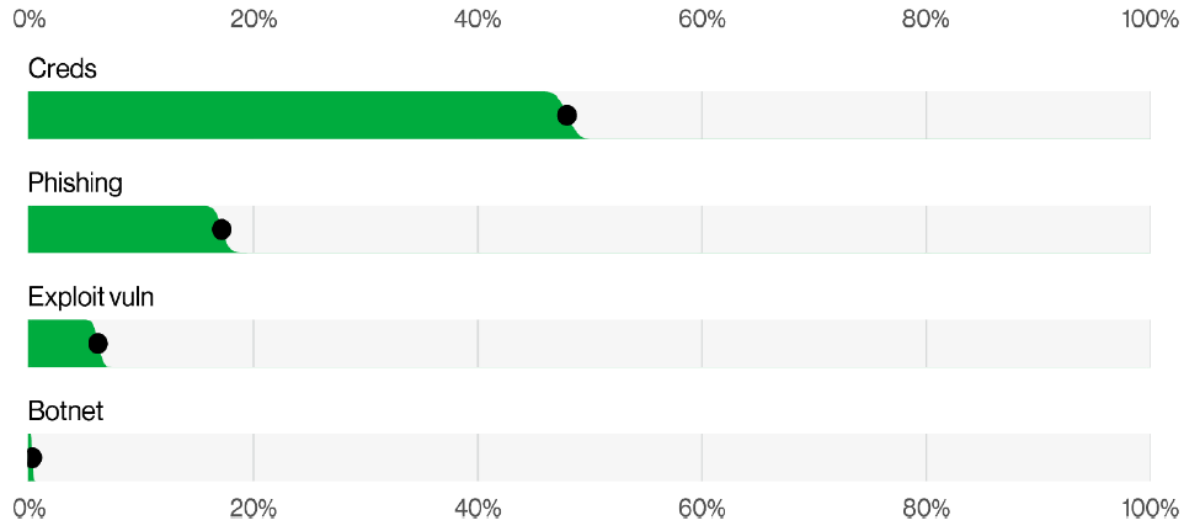


4

Complex, Multi-Stage Lures (Ransomware Setup)



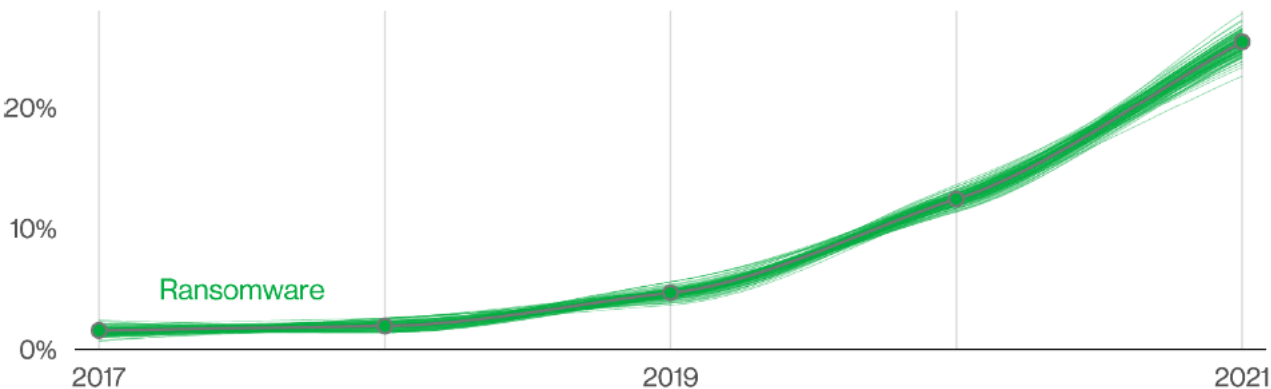
2022 Verizon DBIR Summary of Findings:



There are four key paths leading to your estate: Credentials, Phishing, Exploiting vulnerabilities and Botnets. These four pervade all areas of the DBIR, and no organization is safe without a plan to handle them all.

Figure 5. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

2022 Verizon DBIR Summary of Findings:



This year, Ransomware has continued its upward trend with an almost 13% increase—a rise as big as the last five years combined (for a total of 25% this year). It's important to remember, Ransomware by itself is really just a model of monetizing an organization's access. Blocking the four key paths mentioned above helps to block the most common routes Ransomware uses to invade your network.

Figure 6. Ransomware over time in breaches

2022 Verizon DBIR Summary of Findings:

- Compromised Supply Chain Partners were contributors to 62% of the Intrusion Incidents

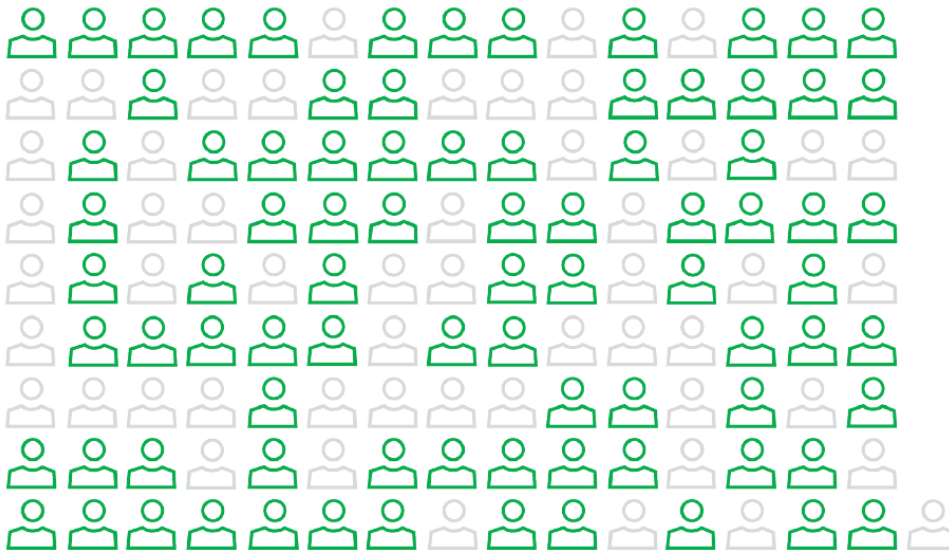
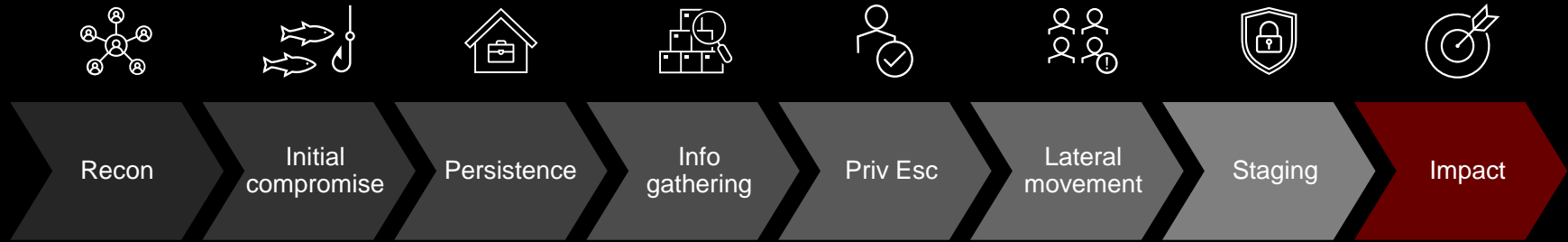


Figure 7. Partner vector in System Intrusion incidents (n=3,403)
Each glyph represents 25 incidents.

How It Plays Out – Typical Cyber Attack Chain



Recon – what happens?

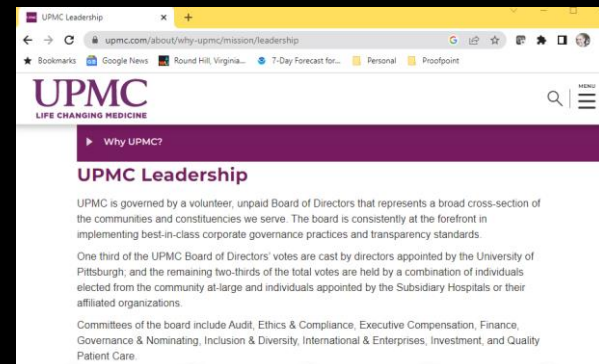


Typical reconnaissance activities include packet sniffing, ping sweeps, port scanning, and internet information queries.

Recon



```
pi@raspberrypi ~  
login as: pi  
pi@192.168.1.131's password:  
Linux raspberrypi 3.2.27+ #250 PREEMPT Thu Oct 18 19:03:02 BST 2012 armv6l  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/*copyright*.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Mon Dec 17 10:59:46 2012 from 192.168.1.6  
pi@raspberrypi ~
```



Initial Compromise Lure – Get Your Vaccine ID from the CDC

United States Centers for Disease Control

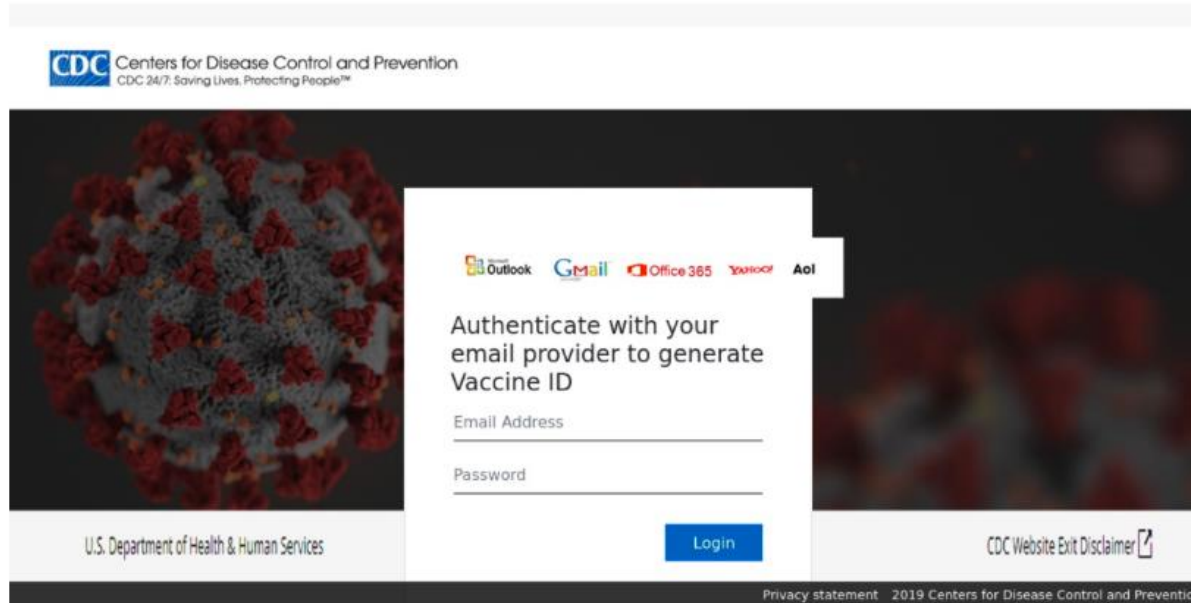


Figure 3: Spoofed CDC Branded Credential Phishing Template via `cdc[.gov].[/coronavirus[.]secure[.]server[.]shorttermrental[.]org`

- Looks very similar to CDC website
- Seeks credentials
- Offers a “Vaccine ID”

Initial Compromise Lure – Get Your Stimulus Check

The Lure

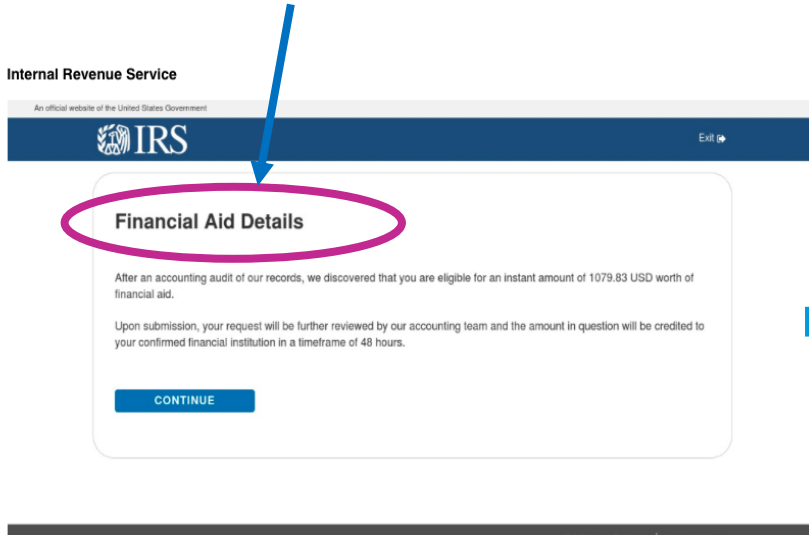


Figure 5 Spoofed IRS Landing Page for Financial Aid via cmattayers[.]com

The Phish

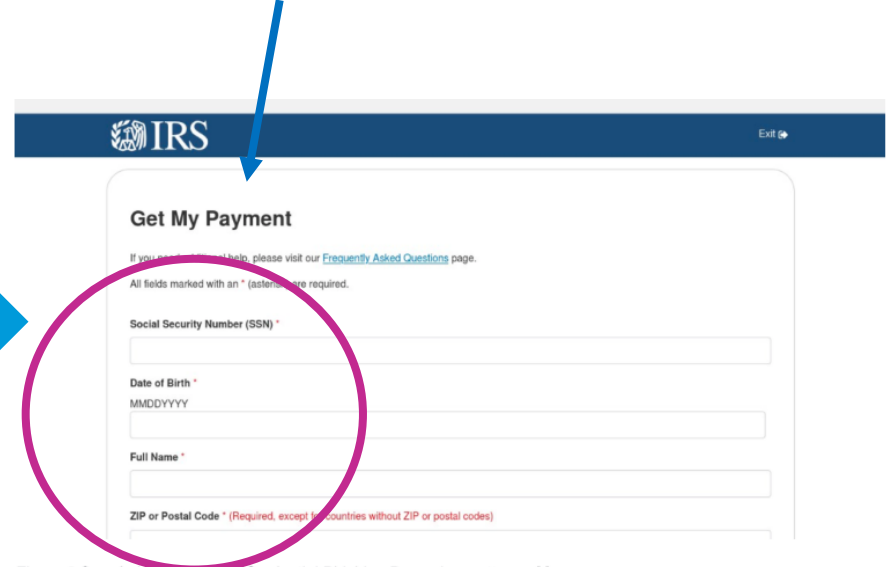


Figure 6 Spoofed IRS Payment Credential Phishing Page via cmattayers[.]com

Request SSN & Date of Birth

Initial Compromise Targeted Attack - IT Service Desk Coronavirus Notice

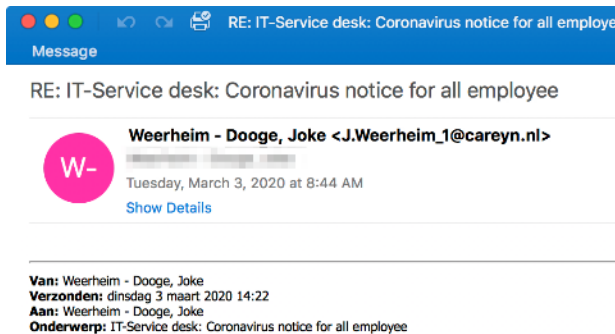
- Emails received with links leading to OWA credential harvesting page

- Proofpoint observed Corona virus notice subject lines purporting to be from an internal IT-Service desk
- The weaponized link in the campaign tricks users into signing up for a mandated seminar or risk disciplinary measures

- **Small Sized Campaign:**

- Targets:
 - More than 400 messages
 - More than 10 customers targeted
 - Hospitals in Healthcare verticals were most impacted by this threat

- **Impact: Stolen Credentials**

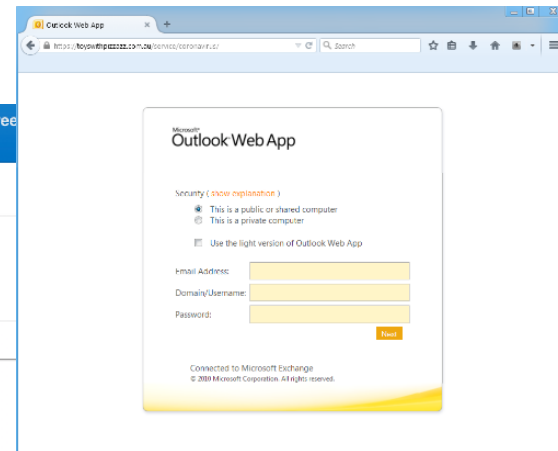


Dear Employee/Staff,

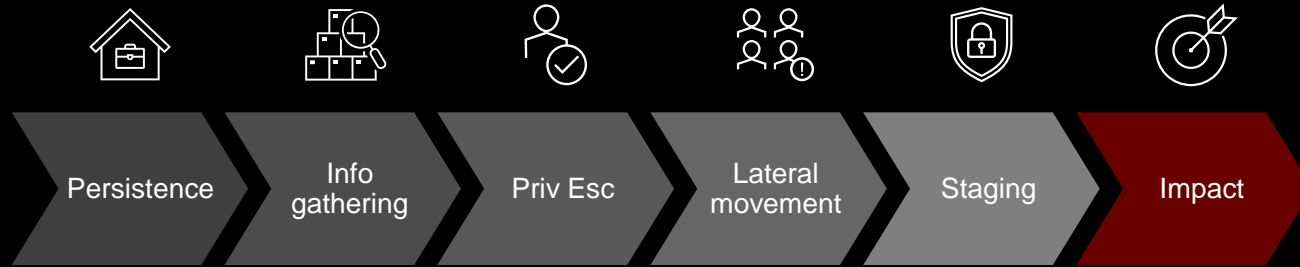
There is an ongoing outbreak of a deadly virus called coronavirus (Covid-19). The virus is spreading like wide fire and the world health organization are doing everything possible to contain the current situation. The virus which originated from china has hit europe, America, Asia and Africa. The government has hereby instructed all organization and institution to educate and enlightened their employee/staff about the virus in order to increase the awareness of the coronavirus (covid-19).

in view of this directives, the institution is currently organizing a seminar for all staff to talk about this deadly virus. All employee/staff are hereby ask to quickly participate in the quick survey to show your awareness about the coronavirus and also register for the seminar. The survey and seminar is compulsory in the battle to win the fight against this epidemic as all employee are Mandated to participate in the survey immediately you receive this notice. Disciplinary measure would be taken on staff that failed to carry out this instruction. Winning this battle is in our collective effort. Kindly follow the link [SURVEY/SEMINAR](#) to participate in the survey and register for the seminar.

Best Regards
IT-Service desk



How It Plays Out – Persistence Through Impact



Persistence - Attackers typically use stolen credentials or malware to get a foothold within the network without being noticed

Info Gathering - Once logged in, they use other tools to find other user vulnerable accounts with more privileged access (**Privilege Escalation**)

Lateral Movement - Once attackers successfully find and login with domain admin type privileges, they can impersonate any user and move freely throughout the enterprise network.

Staging – Using a highly privileged account, the threat actor can install any software backdoor they want

Impact – The attacker leaves with data (**exfiltration**) and/or locks access to applications and data (**ransomware**)

Ransomware Attack Example – [Ortho Virginia](#)

Healthcare IT News

Two years ago, Virginia's largest provider of orthopedic medicine and therapy, OrthoVirginia, was hit with a [Ryuk ransomware attack](#) that disabled access to workstations, imaging systems needed for scheduled surgeries, backed-up data and more.

The initial compromise for the attack = *personal* E-mail!

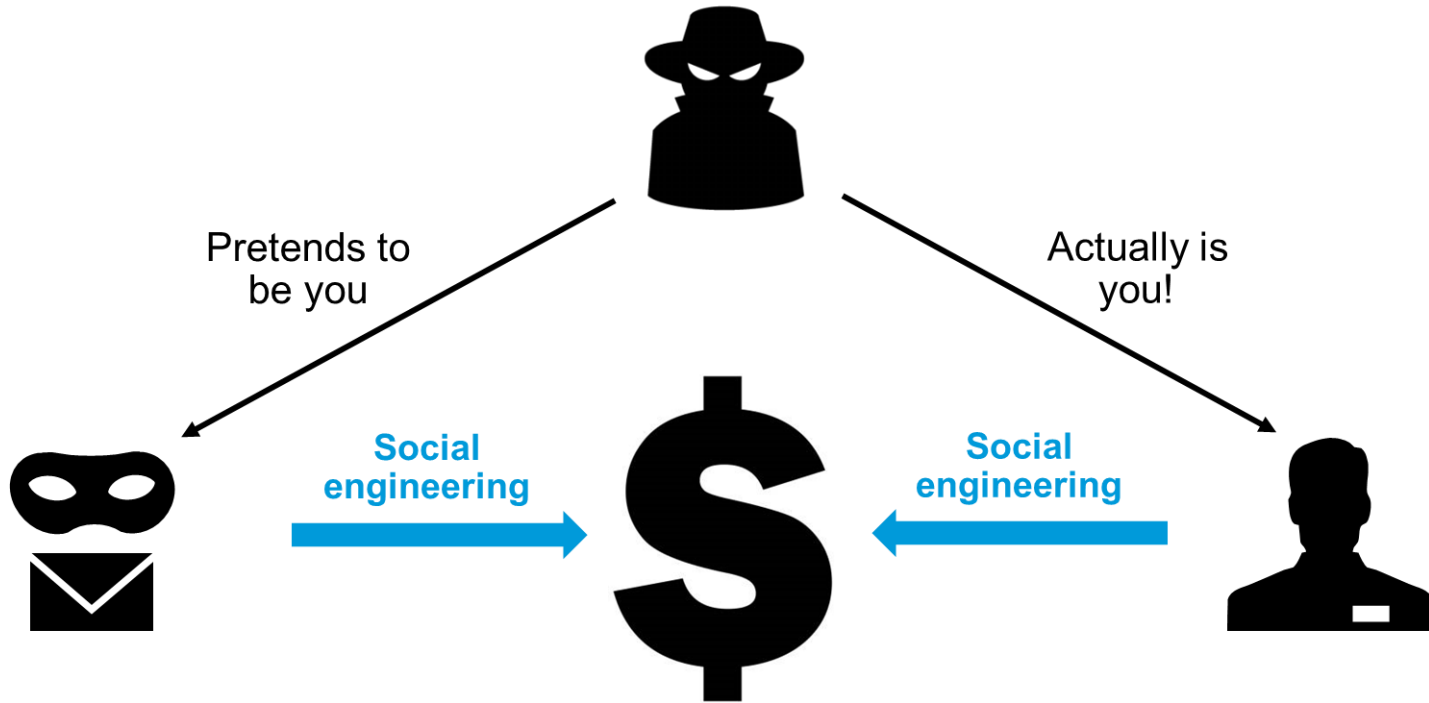
Per Steve Cagle, CEO of Clearwater Security and Compliance, who helped Ortho VA recover:

- People are the number one vector for cyberattacks, and phishing/social engineering is a top threat. It is important to train your workforce to trust nothing and no one when it comes to the digital communication they receive, which now includes voicemails, text messages and phone calls. They need to learn to operate out of skepticism, doubting anything they can't verify as legitimate, including QR codes.
- It's also crucial to test the effectiveness of that training with periodic phishing and social engineering exercises, where you're sending a simulated smishing or vishing to see if/how many of your employees click or respond in ways they shouldn't. This validates the effectiveness of your training and identifies any gaps that need to be filled.



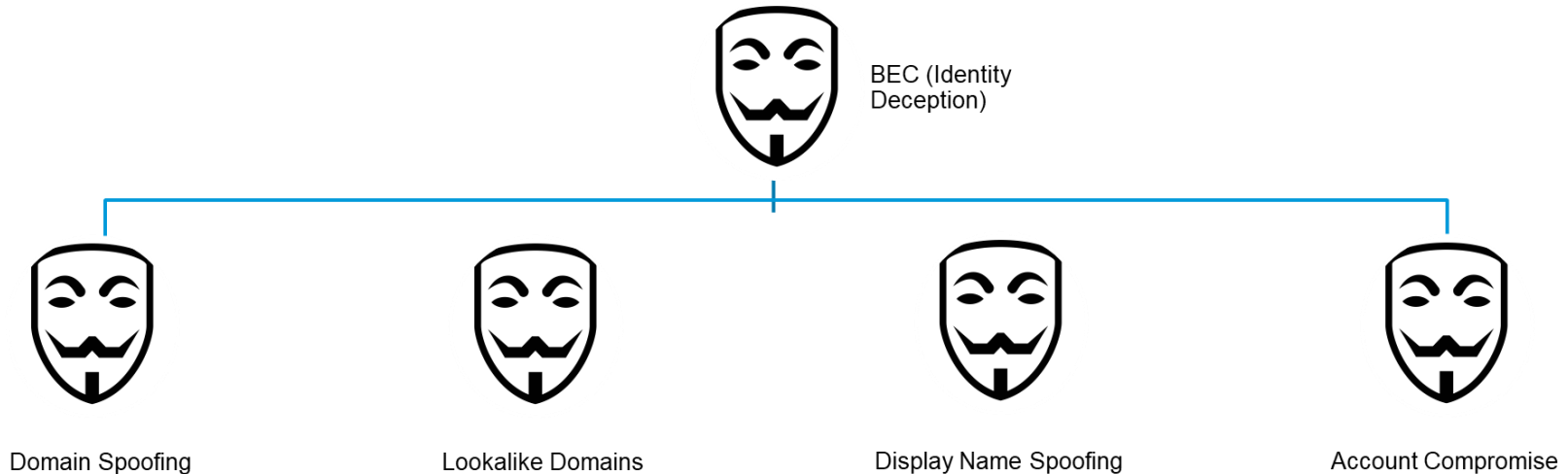
Business Email Compromise (BEC) Impact on Healthcare

BEC Defined - Fraudsters Pose as Someone the Target Trusts



Common BEC Tactics

- Business Email Compromise (BEC)



*Also known as Email Account Compromise (EAC)**

More and More BEC Variants



Gift Carding



Payroll Redirect or
Payroll Diversion



Supplier Invoicing
Fraud



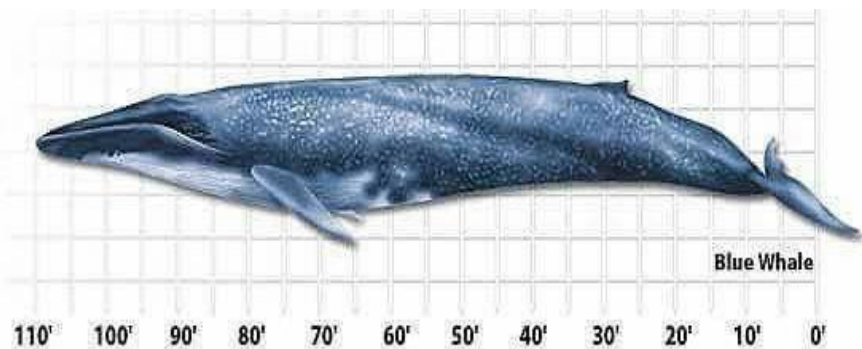
M&A Fraud



Shipment
Redirect

Supply Chain is Healthcare's Largest Cyber Challenge

Supplier Fraud



Blue Whale

Other BEC variants



Killer Whale (Orca)

Average healthcare organization received



200K emails from over

10K different domains

98% received an email-based threat

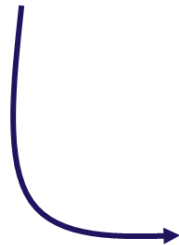


97%

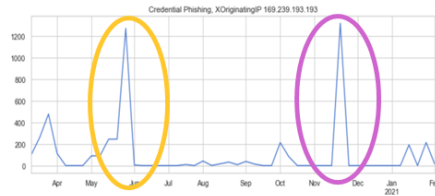
of monitored healthcare organizations have received a threat from a supplier domain via impersonation or BEC

Source: Proofpoint/HIMSS: Addressing supply chain risk and patient safety, 2021

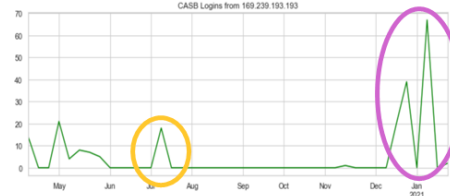
Common Attack Pattern



Cred Phish Campaigns



Compromised Accounts



Hundreds
Other companies targeted

Medical Supplier



United States Department of Justice

THE UNITED STATES ATTORNEY'S OFFICE

NORTHERN DISTRICT *of* GEORGIA

HOME

ABOUT

NEWS

MEET THE U.S. ATTORNEY

DIVISIONS

PROGRAMS

U.S. Attorneys » Northern District of Georgia » News

Department of Justice

U.S. Attorney's Office

Northern District of Georgia

SHARE

FOR IMMEDIATE RELEASE

Tuesday, April 20, 2021

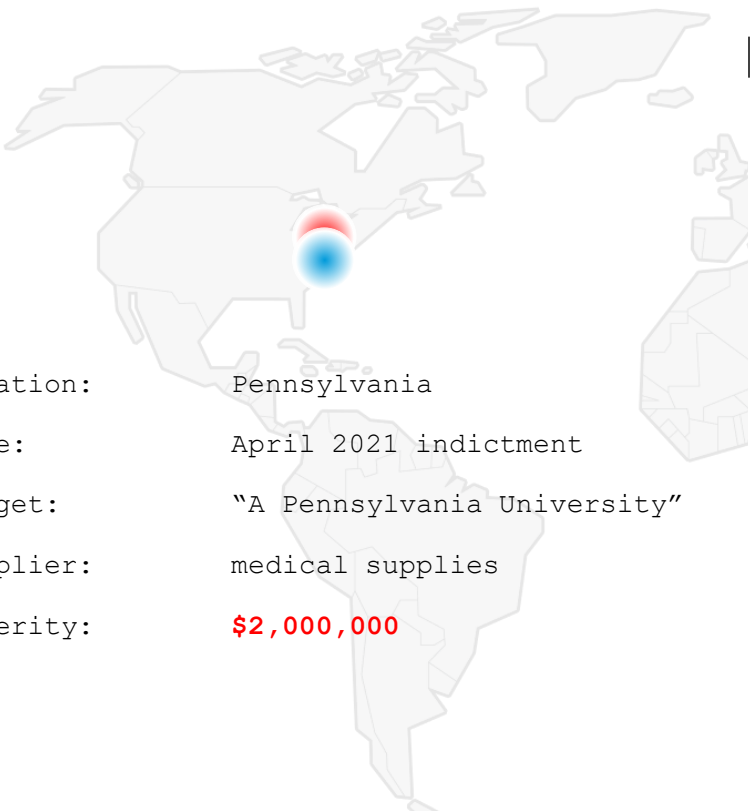
Powder Springs man indicted for laundering over two million dollars in proceeds from a Business Email Compromise scheme

ATLANTA - Denis Onderi Makori has been indicted on charges relating to a business email compromise (BEC) scheme targeting a Pennsylvania university and allegedly defrauding it out of more than \$2 million.

"Business email compromise schemes pose a severe risk of financial loss to public and private institutions alike," said Acting U.S. Attorney Kurt R. Erskine. "In this case, Makori allegedly helped orchestrate a scheme that caused a university to transfer unknowingly over \$2 million to bank accounts he controlled."

"BEC schemes like this alleged one are a big reason why the Georgia Cyber Fraud Task Force, comprised of federal, state and local agencies, was launched in February," said Chris Hacker, Special Agent in Charge of FBI Atlanta. "It takes a combination of education and our priority to investigate and prosecute these cases to make it a deterrent to those who contemplate committing these crimes."

According to Acting U.S. Attorney Erskine, the indictment, and other information presented in court: Various individuals allegedly engaged in a fraudulent BEC scheme to cause a university located in Pennsylvania to send payments totaling more than \$2 million via Automated Clearing House (ACH) to a bank account controlled by Makori, rather than to the intended beneficiary of such payments, a medical supply company based in Alpharetta, Georgia.



Location: Pennsylvania
Date: April 2021 indictment
Target: "A Pennsylvania University"
Supplier: medical supplies
Severity: **\$2,000,000**

Medical Device Manufacturing Category

Diabetes Care

Location: Global

Date: Current

Target: LifeScan

Partner: Platinum Equity

Objective: steal money

Severity: **extreme**

TTPs: Spear Phishing attempt
no account compromise

From: Look alike Partner Accounts Payable

To: CFO

Subject: Payment not received

Payment supposedly late

Result:

CFO follows the process to do some checking and verifying away from automated processes.

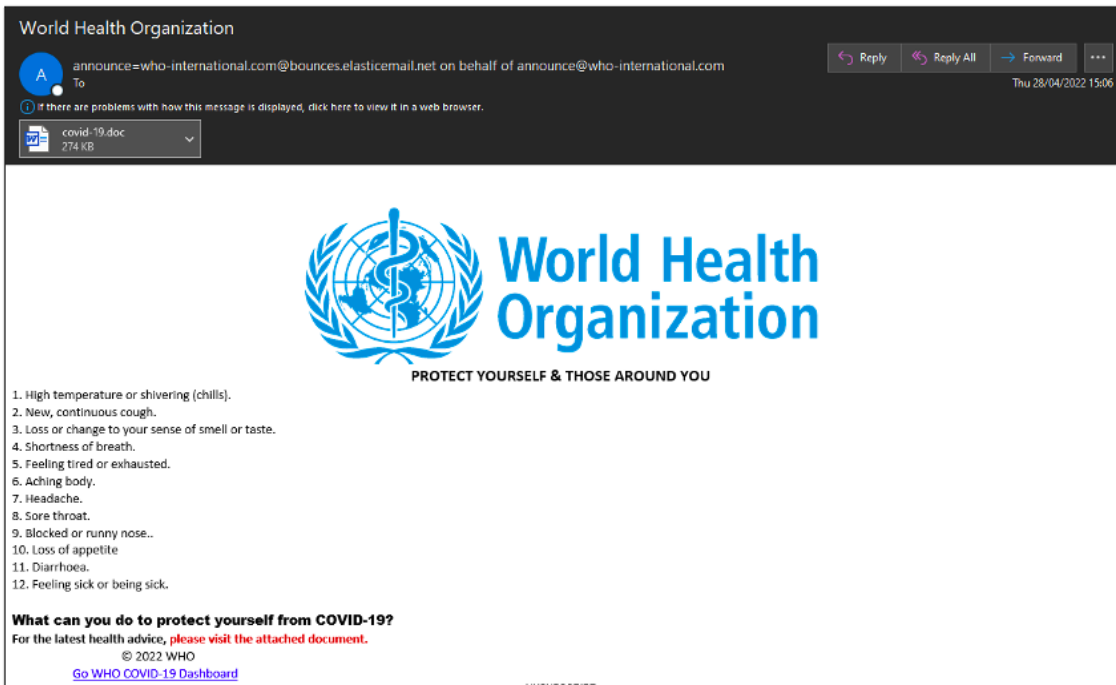
Informed Security of the attempt and investigation happened.

No money was transferred.

Additional steps to block bad actor emails and domains.

Impostor Email from the “World Health Organization”

- Starting April, 2022
- Nerbian RAT
- 64-bit cross-platform malware variant written in Go
- Dropped in smaller phishing campaigns.
- Impersonates the World Health Organization and purports to be sending COVID-19 information to the targets.




Lure – Purchase Order for PPEs

Face Mask Order - Temporary Items


Message

Face Mask Order

 [Redacted Name]

Wednesday, March 25, 2020 at 11:52 PM

[Show Details](#)

 **Face Mask Order**
0.4 KB

[Download All](#) [Preview All](#)

Good Day [Redacted]

Please see attached purchase Order and guaranteed specification for your reference.

Kindly provide us your proforma invoice so we may proceed with payment

Hopping for your soonest response

Thank You

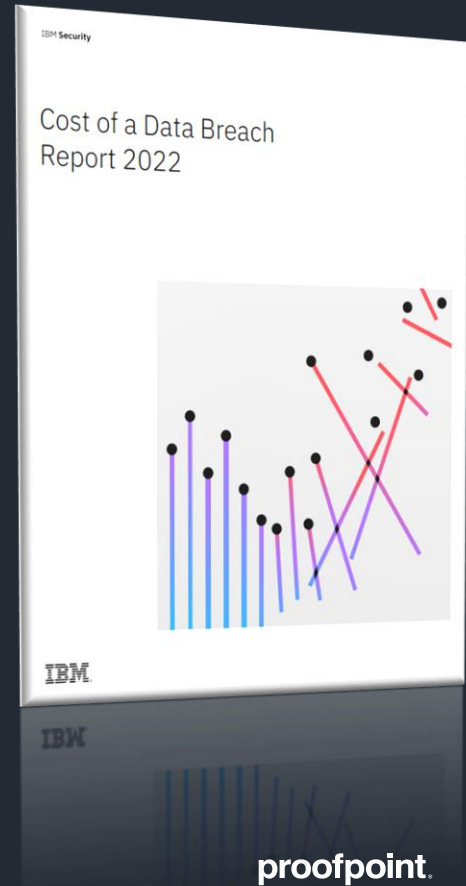
Best Regards

Saludos.
Corporativo Aduanal Nayef SA de CVHeriberto Lopez CastilloTelefono Nextel. 52(867) 192-0723

Why It's Important: More Detail on Impact to Healthcare



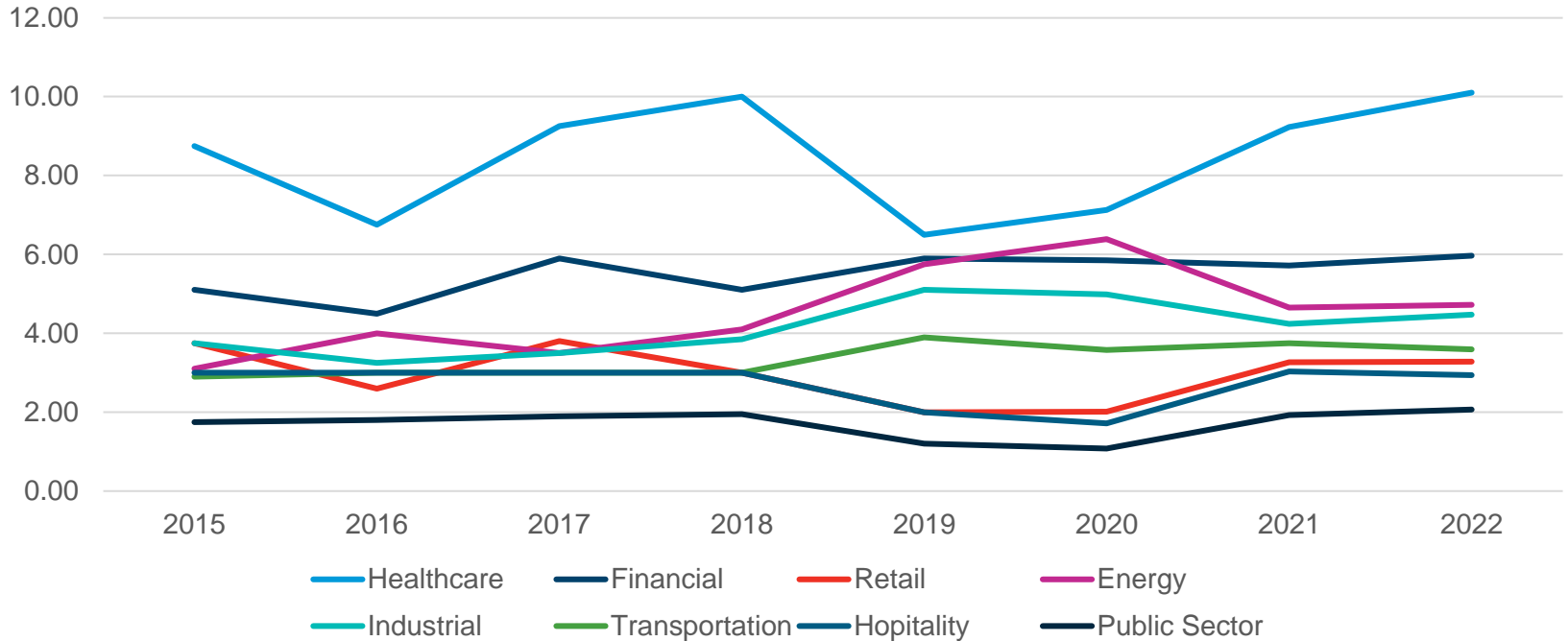
Cybersecurity State of the Union –2022 IBM Cost of a Data Breach Report



Average Total Cost of Data Breach Per Industry

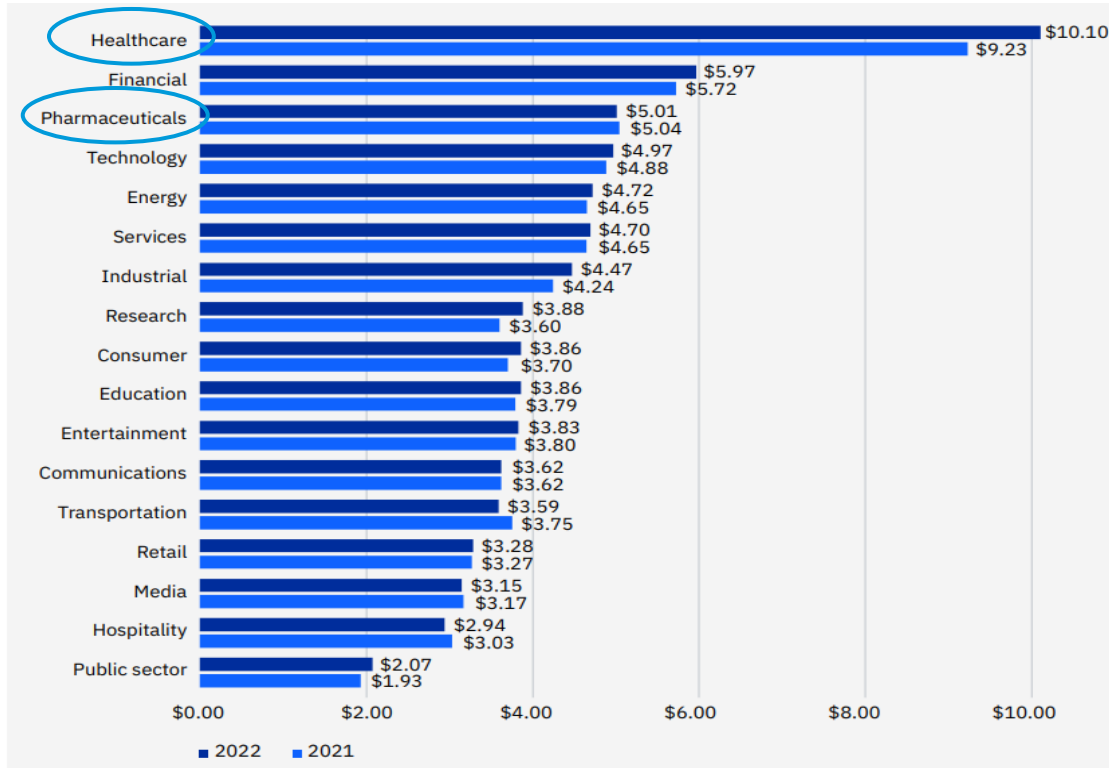
\$US Millions

2022 IBM Ponemon
Cost of a Data Breach Report



Average Total Cost of Data Breach by Industry

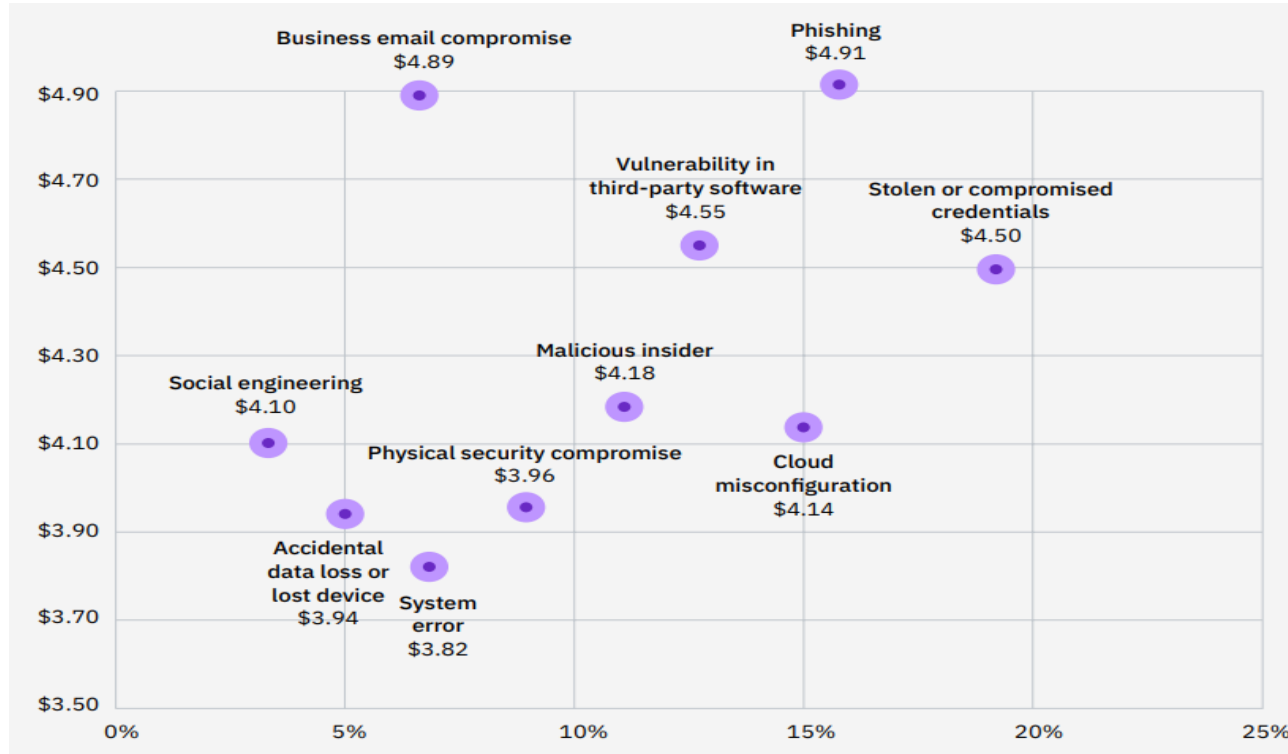
Measured in US\$ Millions



2022 IBM Ponemon
Cost of a Data Breach Report

Average Cost and Frequency of Data Breaches by Initial Attack Vector

Measured in US\$ Millions



2022 IBM Ponemon
Cost of a Data Breach Report

DIY Activities

Given what you've learned, what would you fix first, second and third if you were a security practitioner?

Check out the HHS Breach Portal:

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf



Part 2: Protection Against Cyber Attacks on Healthcare

proofpoint

Mike Yriart

Senior Account Manager – HealthCare

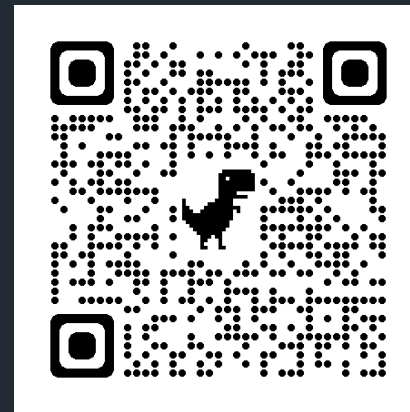


DIY Activities from Part 1:

1) *What would you fix first, second and third if you were a security practitioner?*

2) *Anything surprising you saw in the HHS Breach Portal?*

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf



Top Three Cybersecurity Risks: All People-centric




85%

INVOLVED A HUMAN ELEMENT

Vast majority of ransomware attacks start with email

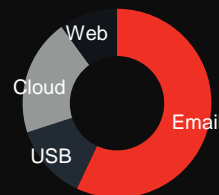
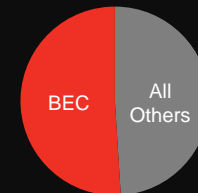
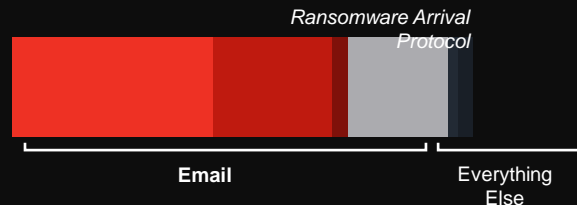
— paloalto research

Business E-Mail Compromise (BEC) losses exceed all other cybersecurity losses combined

—  data for 791,790 incidents

99% of data loss incidents are human-driven

— proofpoint data across 3,000 organizations



And in Healthcare? All People-centric



Top 3 threats

INVOLVED A HUMAN ELEMENT

Phishing attacks
(57% of respondents)

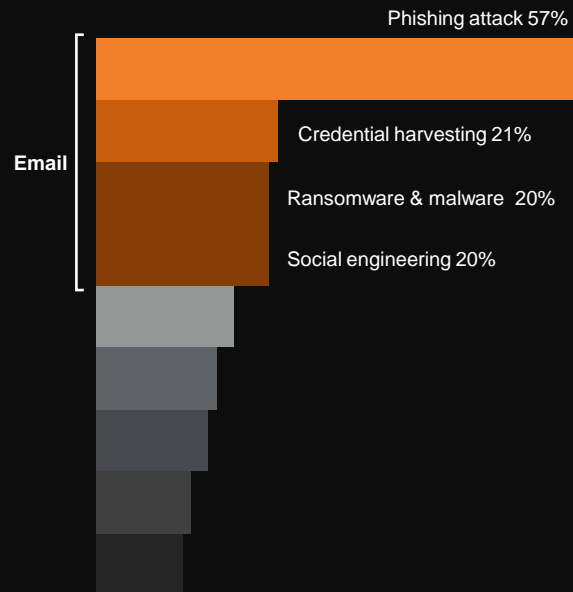
—  HIMSS research

Credential harvesting attacks
(21% of respondents)

—  HIMSS research

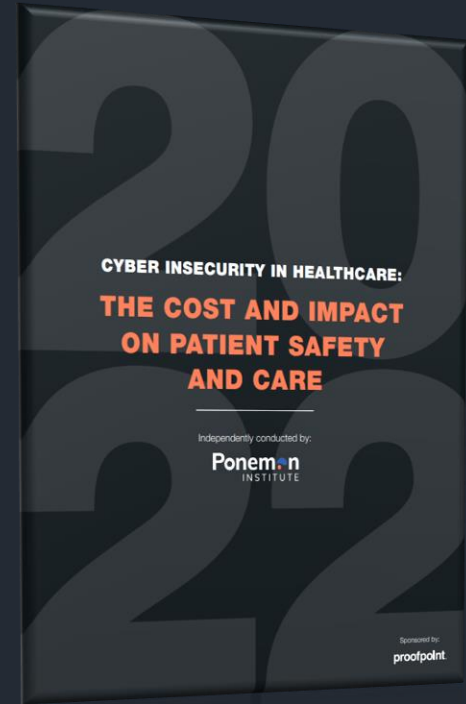
Social engineering & ransomware
(20% of respondents)

—  HIMSS research





Cybersecurity State of the Union – 2022 Cyber Insecurity in Healthcare Ponemon Report



Cyber Insecurity & The Impact on Patient Care

With sponsorship from Proofpoint, Ponemon Institute surveyed 641 IT and IT security practitioners in healthcare organizations who are responsible for participating in cybersecurity strategies including setting IT cybersecurity priorities, managing budgets and selecting vendors and contractors.



89%

of organizations in this research had at least one cyberattack over the past 12 months



\$4.4M

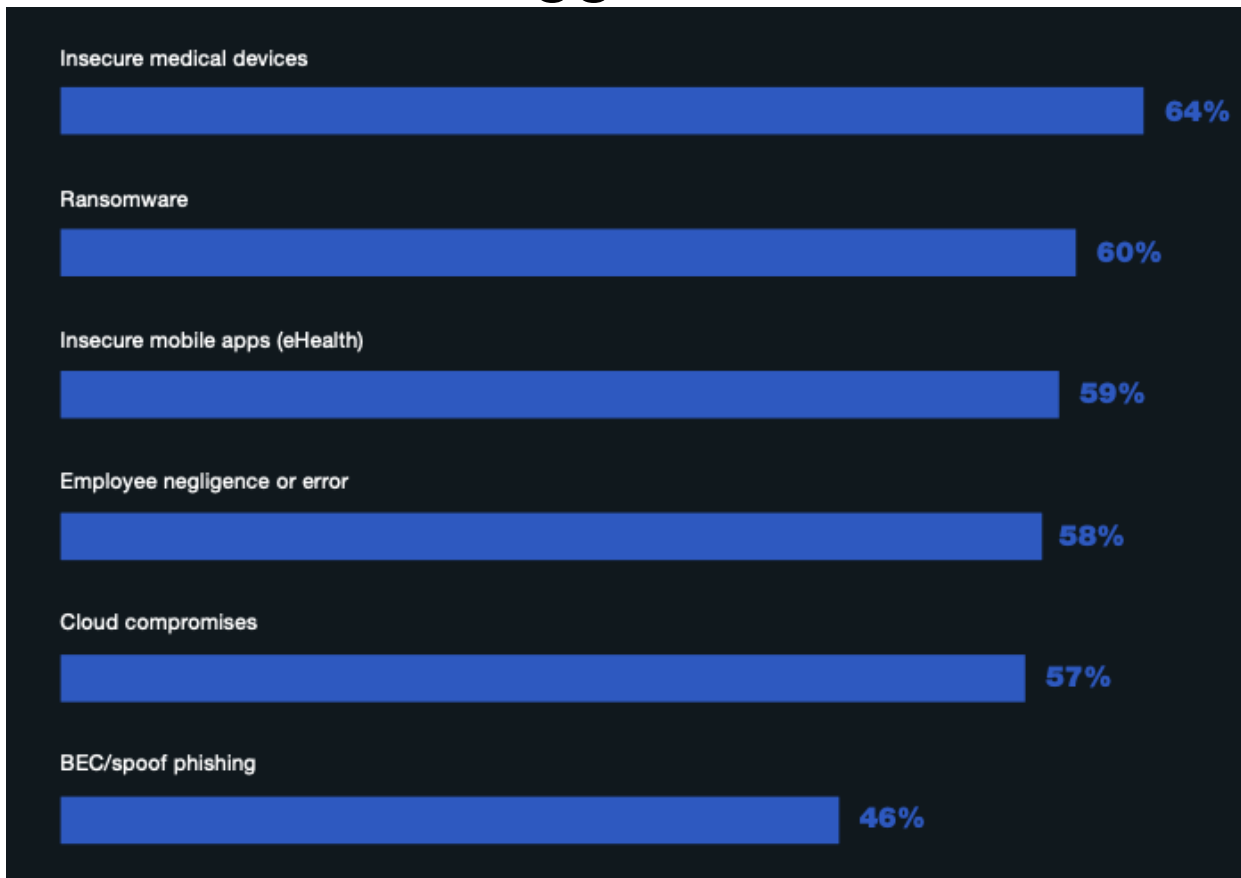
The average total cost for the single most expensive cyberattack experienced over the past 12 months



\$1.1M

in lost productivity was on average the most significant financial consequence from the cyberattack

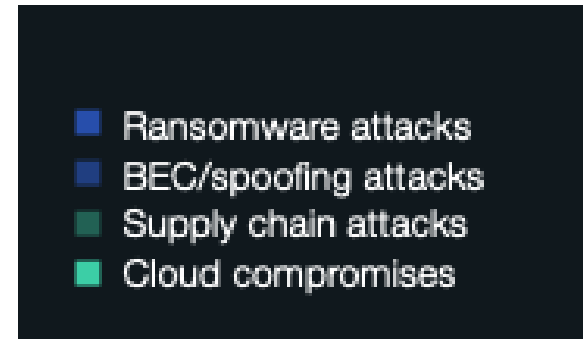
Current Threats of Biggest Concern



Cyber Attacks That Have Actually Disrupted Patient Care



...And Adversely Impacted Patients



What are the ways to protect Healthcare?

General Security Components to Defend at Each Attack Stage:

Protect Against
Initial Compromise

Stop Discovery,
Lateral Movement
& Persistence

Prevent Data
Exfiltration or
Destruction

- Firewall
- Web Application Firewall
- Endpoint / Virus Protection
- Vulnerability Scanning
- Patch Management
- Identity Management
- Secure E-mail Gateway
- DMARC
- Malicious Mail Pull-Back / Retrieval
- Security Awareness Training
- Phishing Simulation
- Web Isolation
- Secure Web Gateway
- Cloud Application Security Broker

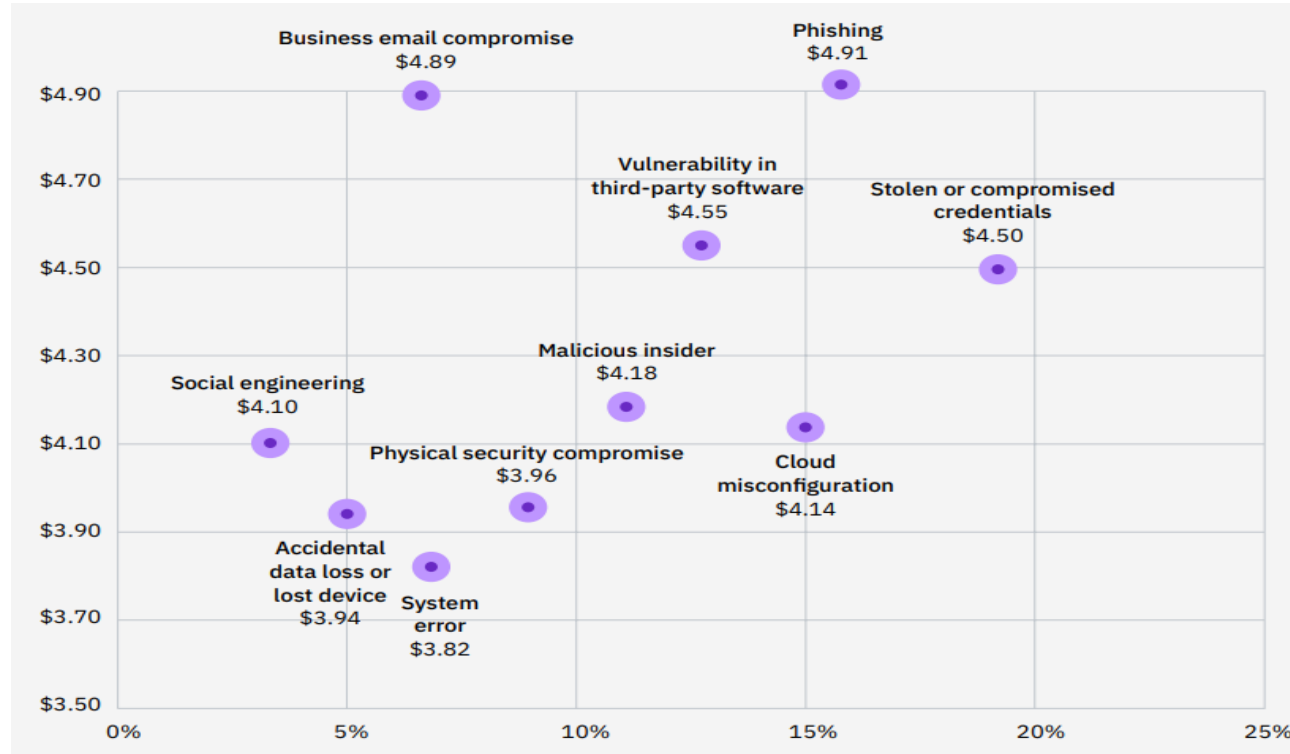
- Firewall
- Web Application Firewall
- Endpoint / Virus Protection
- Cloud Application Security Broker
- Secure Web Gateway
- Zero Trust Network Access
- Identity Threat Detection & Response

- Immutable Data Backups
- E-mail Archiving
- Security Awareness Training
- Cloud DLP (CASB)
- Endpoint DLP
- Insider Threat Management (ITM)
- E-mail DLP
- Web Isolation
- SaaS Isolation
- Secure Web Gateway
- Zero Trust Network Access (ZTNA)

Where should we start?

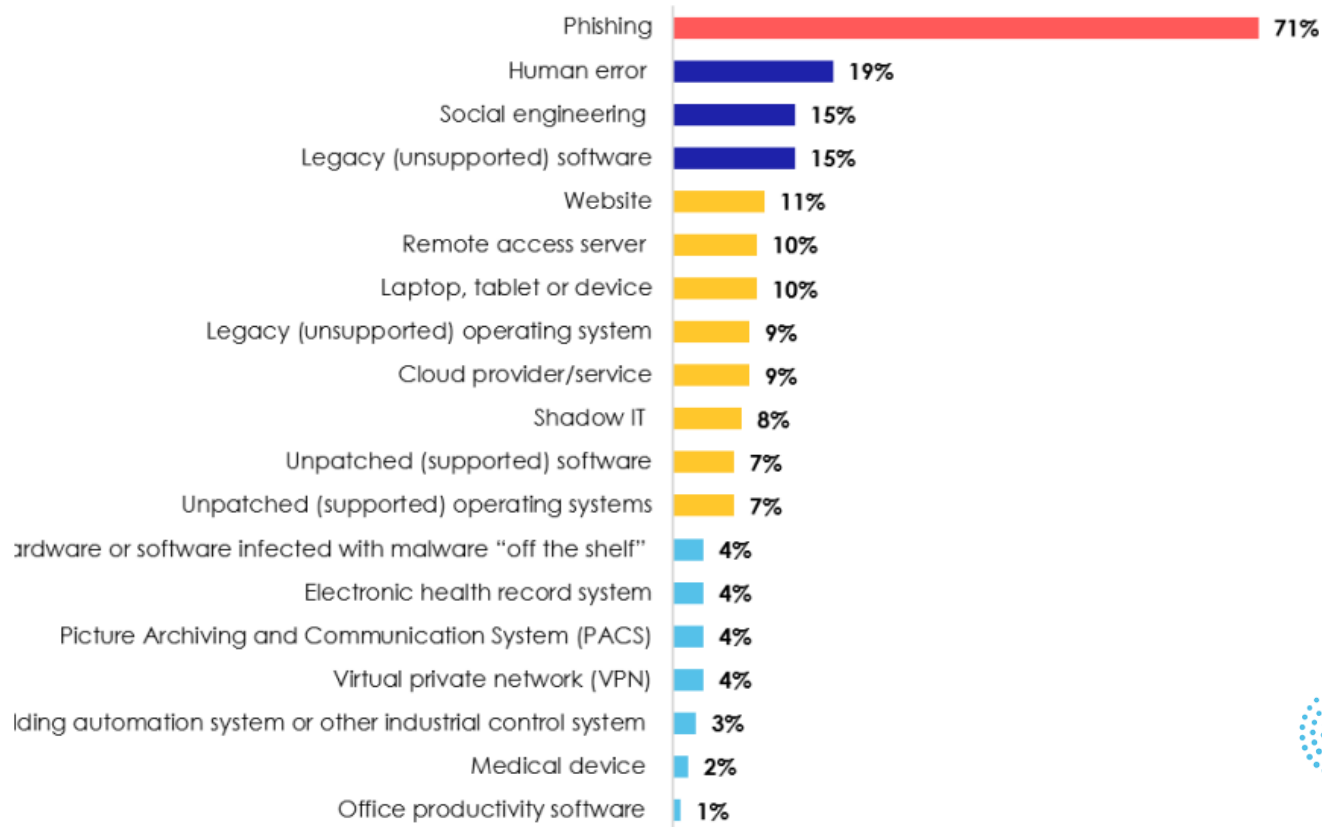
Refer back to this: Average Cost and Frequency of Data Breaches by Initial Attack Vector

Measured in US\$ Millions



2022 IBM Ponemon
Cost of a Data Breach Report

And Refer back to this: The Initial Points of Compromise Ranked



What are all these things?



Secure E-mail Gateway and related technologies

- A secure email gateway is a system that filters and monitors incoming and outgoing email traffic, enforcing security policies, and protecting against various threats such as spam, malware, phishing attempts, and data leaks.
- A variety of choices exist, from basic giving low efficacy, to the more comprehensive, which leverage AI for filtering, and offer more features for advanced threat protection, pulling back post-delivery weaponized mail, data loss prevention, and detection of zero-day threats.



Identity Threat Detection and Response

- Identity threat detection and response (ITDR) is a security mechanism to identify identity vulnerabilities and help remediate them. It can also detect when identities are being used as part of a cyber attack and halt the attacker.
- ITDR is a critical component of any comprehensive cybersecurity strategy, because so many cyber attacks require credentials to work. By protecting identities, organizations can drastically cut the attacker's ability to gain access to sensitive data or systems.



Cloud Application Security Broker

- A security solution that helps organizations control and secure their cloud usage. CASBs can help organizations to:
 - Enforce security policies on cloud usage, like use of third-party apps
 - Protect sensitive data in the cloud
 - Detect and respond to cloud-based threats



Vulnerability Scanning & Management

- Vulnerability management is the process of identifying, assessing, and mitigating vulnerabilities in an organization's IT assets. Vulnerability management can help organizations to:
 - Reduce the risk of data breaches and other security incidents
 - Improve compliance with security regulations
 - Protect their IT assets from attack
- Vulnerability management is an ongoing process, and it is important to continuously monitor for new vulnerabilities and to update security controls as needed.

So how can Proofpoint help?

Break the Attack Chain & Address Risks that Matter Most

- This is where **Proofpoint** focuses



Recon

Initial compromise

Persistence

Info gathering

Priv Esc

Lateral movement

Staging

Impact

ROLE: Finance

ROLE: Research Scientist

ROLE: Support Contractor



Interacts with risky suppliers

Can move money

Fully remote

Part of works council

Collaborates externally via cloud apps

Targeted via alias

Clicks everything

Handles customer data



Service Accounts



Local Admin Accounts



Shadow Admin Accounts



Exposed Credentials & Cloud Tokens
Legacy App Accounts



Open RDP Sessions



Open RDP Sessions



CARELESS USER



COMPROMISED USER



MALICIOUS USER

Threat Education & Blocking

Identity Threat Detection + Response

Information Protection

PEOPLE ARE COMPLEX, DIFFERENT

ROLE: Nursing Contractor

Targeted via
alias



Clicks
everything

Handles
patient data

ROLE: Physician

Collaborates
externally via
cloud apps



Remote
&
On site

Part of
education
consortium

ROLE: Finance

VAP



Interacts
with risky
suppliers

Can move
money

PROTECTION FOR PEOPLE, HOW AND WHERE THEY NEED IT

ROLE:

Nursing Contractor

Isolate all links to shared alias so clicks do no harm



Use DLP & ITM to protect patient data

Train on patient data handling

ROLE:

Physician

Deliver custom training on campaigns targeting research & PHI



Web isolation to preserve privacy

Protect cloud collaboration with web, endpoint DLP

ROLE:

Finance

Block impostor attacks with ML



Flag risky suppliers with tags

Train on BEC threats

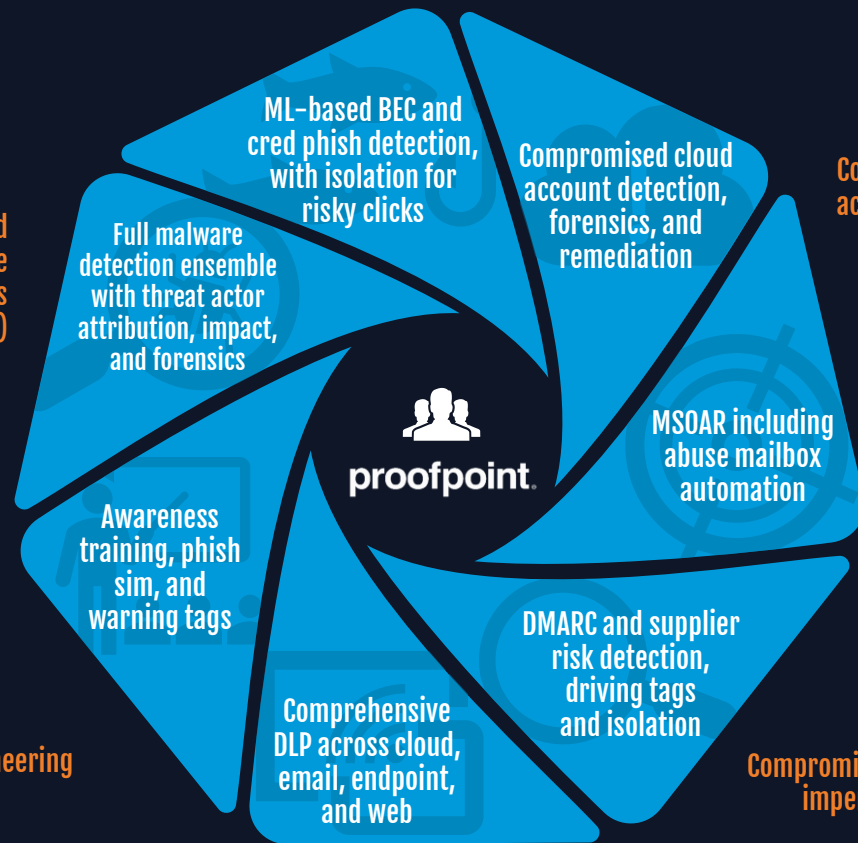
PLATFORM APPROACH: THE RIGHT PROTECTION FOR THE RIGHT PEOPLE

“The evolution in threats has led to increased demand for other techniques and services, such as DMARC, cloud access security broker (CASB)/API integrations, continuous awareness and mail-focused security orchestration, automation and response (MSOAR).”

Gartner

User-activated
Malware
(attachments
& URLs)

Social engineering



Data theft

PROOFPOINT KEY CAPABILITIES

- E-mail Protection / Gateway
- Compliance & Archiving
- E-mail Fraud Defense (managed DMARC/DKIM/SPF)
- Secure E-Mail Relay
- Identity Threat Detection and Response
- Browser & SaaS Isolation
- Phishing Simulation & Security Awareness Training
- Sensitive Data Discovery, Classification & Tagging
- Data Loss Prevention & Cloud Security
- Secure Web Gateway & Zero Trust Networking

Proofpoint Platform Components to Defend at Each Attack Stage:

Protect Against
Initial Compromise

- Proofpoint Protection Server (PPS)
- E-mail Fraud Defense (EFD)
- Targeted Attack Protection (TAP)
- Threat Response Auto-Pull (TRAP)
- Proofpoint Security Awareness Training (PSAT)
- Isolation
- Closed Loop E-mail Analysis & Response (CLEAR)
- Cloud Application Security Broker (CASB)

Stop Discovery,
Lateral Movement
& Persistence

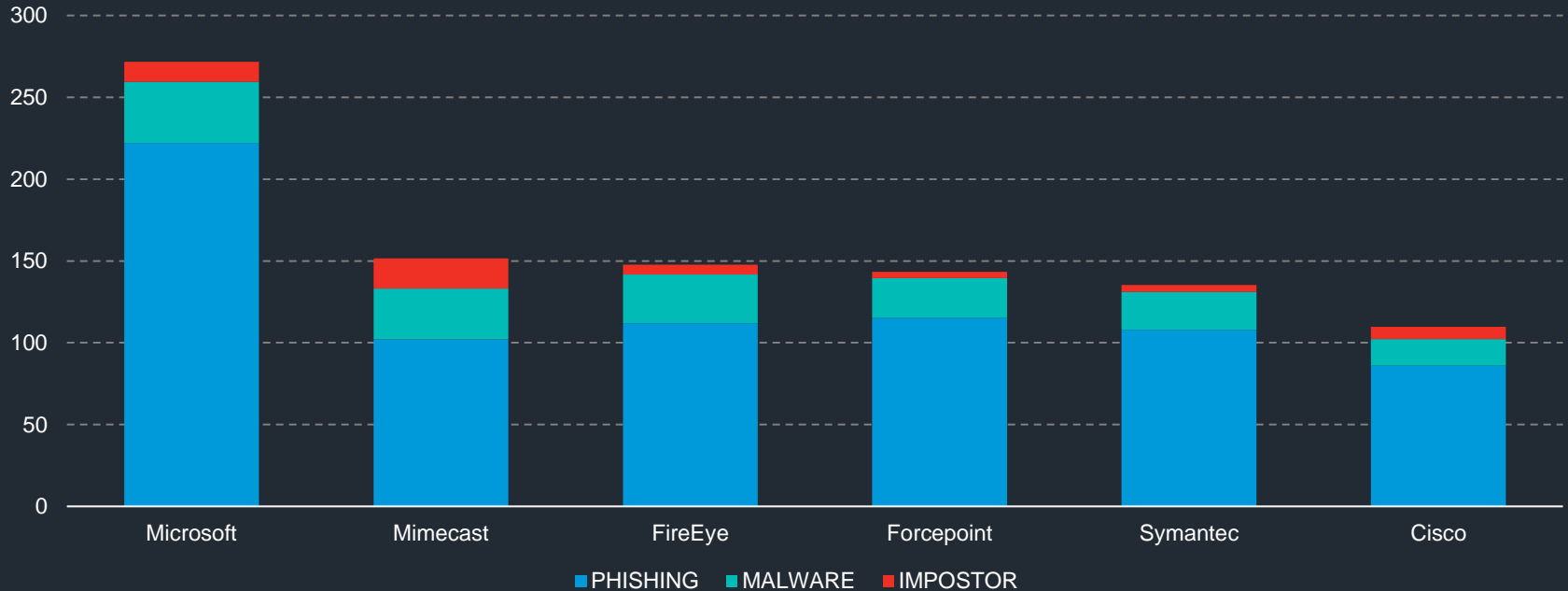
- Cloud Application Security Broker (CASB)
- Proofpoint Secure Web Gateway
- Zero Trust Network Access (ZTNA)
- Identity Threat Detection & Response (Illusive)

Prevent Data
Exfiltration or
Destruction

- Proofpoint Security Awareness Training
- Archiving
- Cloud DLP(CASB)
- Endpoint DLP
- Insider Threat Management (ITM)
- E-mail DLP
- Isolation
- SaaS Isolation
- Proofpoint Secure Web Gateway
- Zero Trust Network Access (ZTNA)

Advanced threats delivered by other vendors during threat assessments in 2022

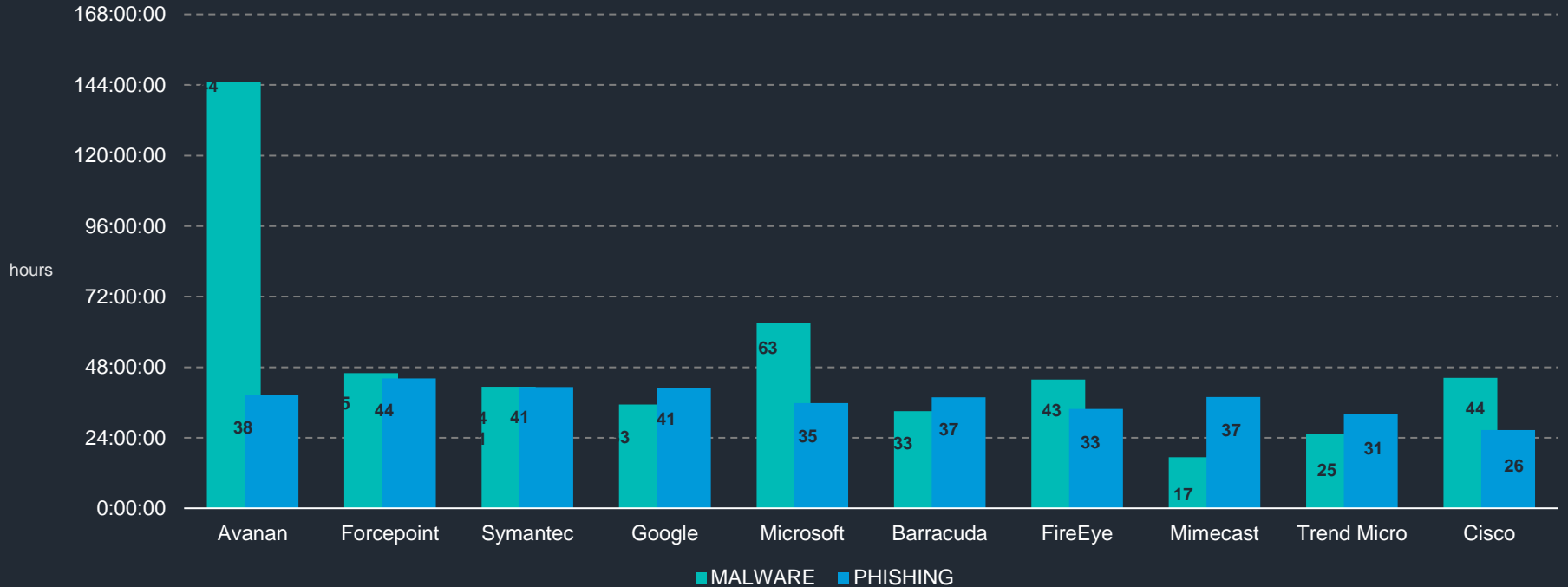
Advanced Threats Detected / 1,000 mailboxes



Proofpoint detected threats hours before the competition

Threats detected by Proofpoint seen delivered by others during threat assessment in 2022

Average Dwell Time (hours)



Financial Implications: Email Security

Benefits – Investment Costs = Business Value

Investment Costs



- This value includes the licensing, professional services, and costs for internal resource time through the deployment.

Risk Resistance



- This risk-adjusted value is based on the probability of experiencing a data breach using an annual rate of occurrence (ARO) of 1 incident per year.

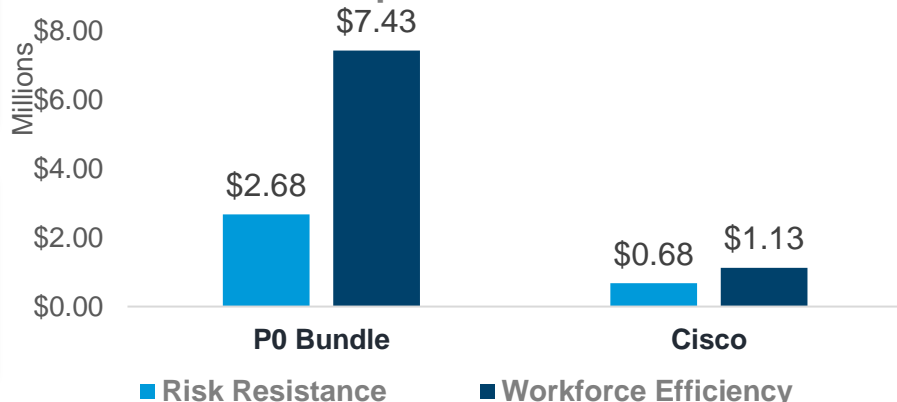
Workforce Efficiency



- Efficiency is representative of a significant reduction in the level of effort to monitor, prevent, and respond to potential threats.

Category	P0 Bundle	Cisco	Diff
Investment Costs			
Risk Resistance	\$2,679,665.80	\$681,632.00	\$1,998,033.80
Workforce Efficiency	\$7,434,842.98	\$1,125,908.67	\$6,308,934.31
Total			

Value Comparison Over Year 1



Proofpoint – Healthcare Overview

The leader in protecting people from advanced threats and compliance risk

78% of healthcare companies in Fortune 500

TOP 8 Of the ten largest U.S. health insurers

70% of top 10 best hospitals



Enhancing knowledge of HC security challenges

HEALTHCARE
CUSTOMER
ADVISORY BOARD



Thank you

The logo for Proofpoint, consisting of the word "proofpoint" in a lowercase, bold, sans-serif font, followed by a registered trademark symbol (®).

Mike Yriart

Title

Senior Account Manager – HealthCare

(571-830-4255)

myriart@proofpoint.com