CLACKAMAS COMMUNITY COLLEGE

INFORMATION SECURITY PROGRAM

Presented by Saby Waraich

COVERED TODAY

A BRIEF OUTLINE

The State of Information Security

Where are we Today

Where do we go Next

Cybersecurity Awareness

Executive Summary

Attackers:
"It ain't broke, so why fix it?"

New threat trends in information security aren't *really* new.

Previously understood attacks still work just fine, and so attacks are simply an evolution, not a revolution.

Traditionally, most organizations are not doing a good enough job of the security fundamentals, which is why attackers have been able to use the same old tricks.

However, information security has finally caught the attention of organizational leaders, presenting the opportunity to implement a comprehensive security program.

Persistent Issues

1 Evolving ransomware

Continual changes in type and platforms make ransomware a persistent threat. The frequency of ransomware attacks was reported last year to have **doubled.**[1]

2 Phishing attacks

Despite filtering and awareness, email remains the most common threat vector for phishing attacks (**96%**), and an average of **4%** of participants in phishing campaigns still click on them.[2]

3 Insider privilege and misuse

Typically **28%** of breaches are often perpetrated by insiders, with **12%** involving privilege misuse.[2] **Takeaway:** Care less about titles and more about access levels.

4 Denial of service

The median amount of time that an organization is under attack from a DDoS attack is three days.[2]

Emerging Trend

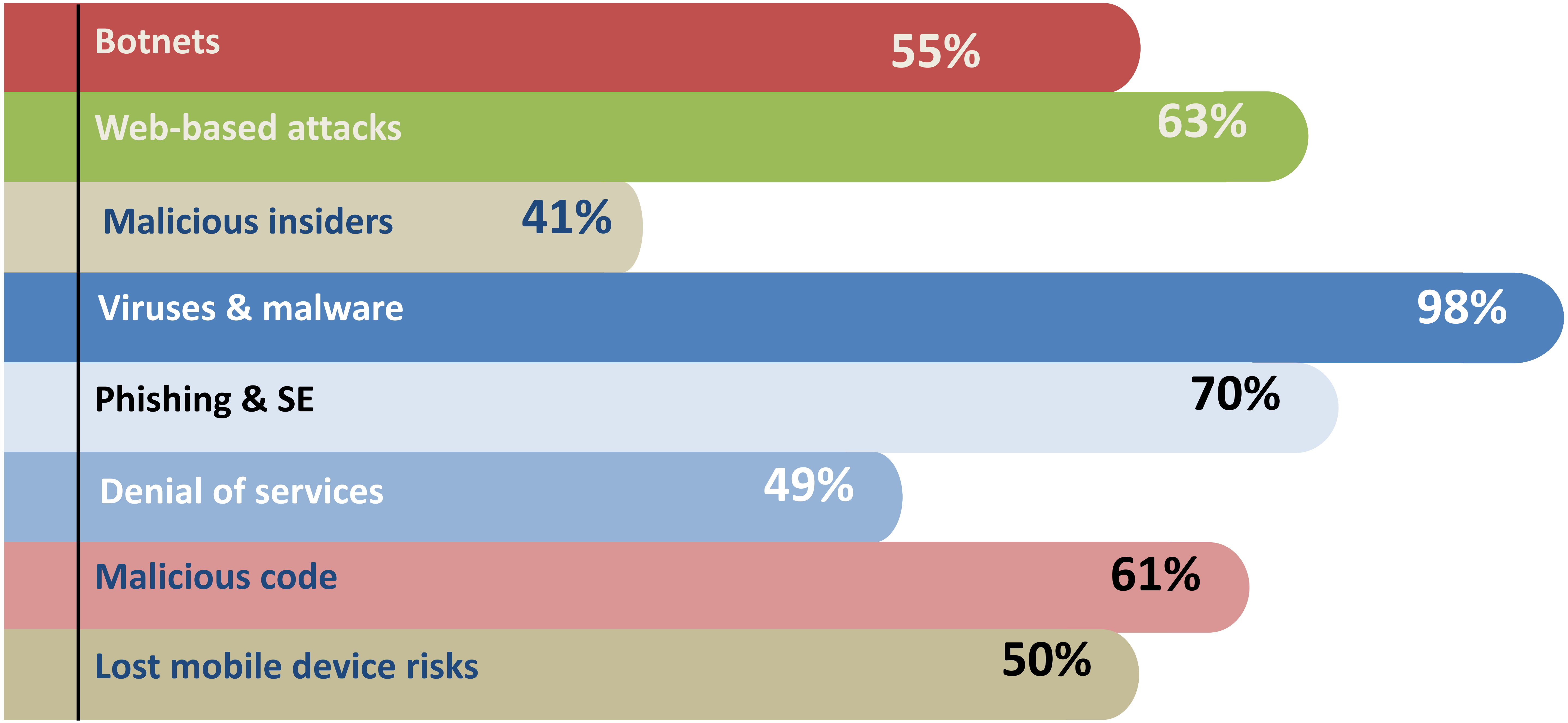
5 Advanced Identity and Access Governance

Utilizing emerging technologies in automation, orchestration, and machine learning, the management and governance of identities and access has become more advanced.[1]

Sources: [1]Ponemon, "2017 Cost of Cyber Crime Study"; [2]Verizon, "2018 Data Breach Investigations Report"

Nearly 100% of companies have been compromised

In 2016, 237 benchmark companies experienced the following frequency and type of attacks:



An attacker must only be successful once.
The defender – you, must be successful every time.

It’s not a matter of *if* you have a security incident, but *when*

ORGANIZATIONS NEED TO EXPECT THE INEVITABLE SECURITY BREACH.

90%

of businesses have experienced an external threat in the last year.[1]

50%

of IT professionals consider security to be their number one priority.[1]

53%

of organizations claimed to have experienced an insider attack in the previous 12 months.[2]

46%

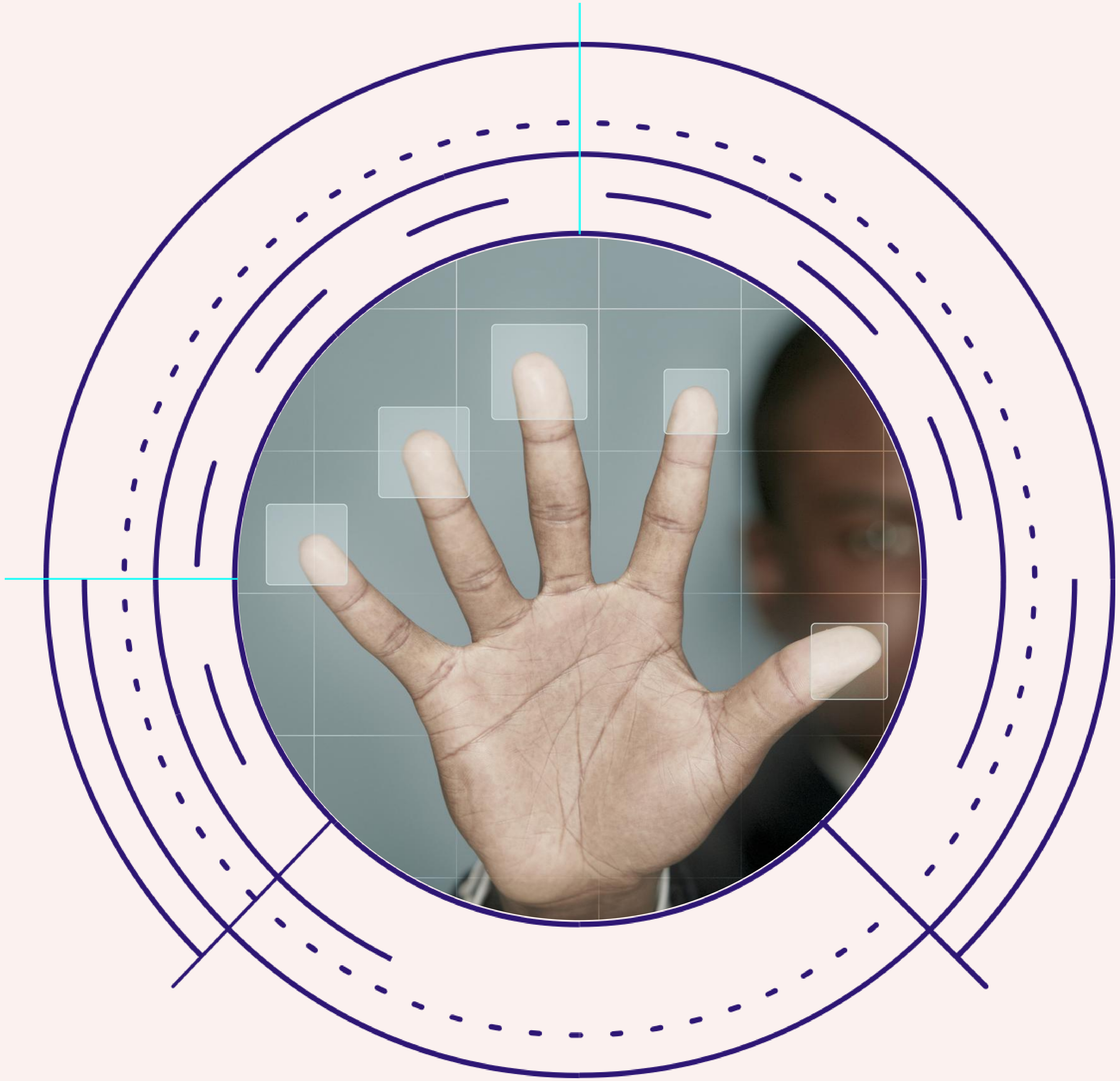
of businesses believe the frequency of attacks is **increasing.**[1]

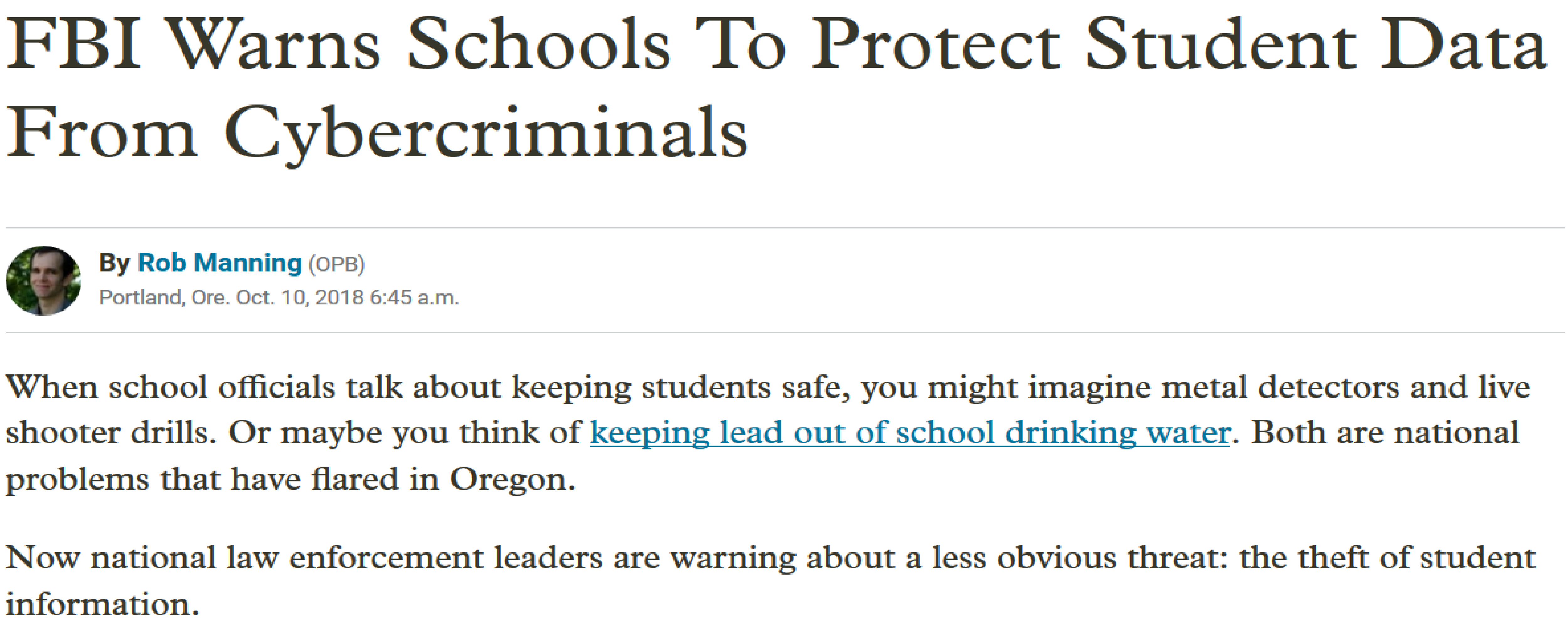
Effective IT leaders approach their security strategy from an understanding that attacks on their organization will occur. Building a strategy around this assumption allows your security team to understand the gaps in your current approach and become proactive vs. reactive.

Sources: [1]Kaspersky Lab, “Global IT Security Risks Survey”; [2]CA Technologies, “2018 Insider Threat Report”

WHERE WE ARE TODAY

Technology sophistication and business adoption, the proliferation of hacking techniques, and the expansion of hacking motivations from financial to now social, political, or strategic motivations have resulted in organizations facing major security risk. Every organization needs some kind of information security program to protect its systems and assets.



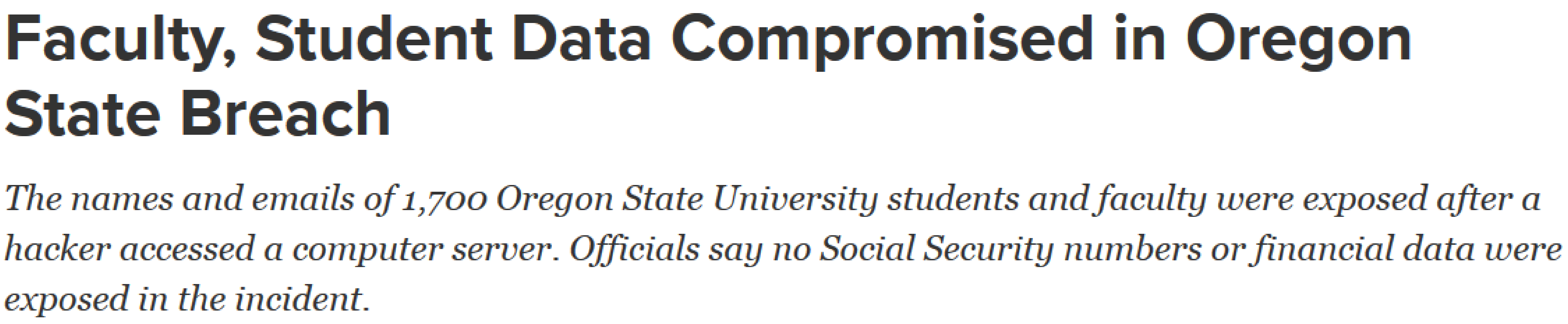


FBI Warns Schools To Protect Student Data From Cybercriminals

By Rob Manning (OPB)
Portland, Ore. Oct. 10, 2018 6:45 a.m.

When school officials talk about keeping students safe, you might imagine metal detectors and live shooter drills. Or maybe you think of keeping lead out of school drinking water. Both are national problems that have flared in Oregon.

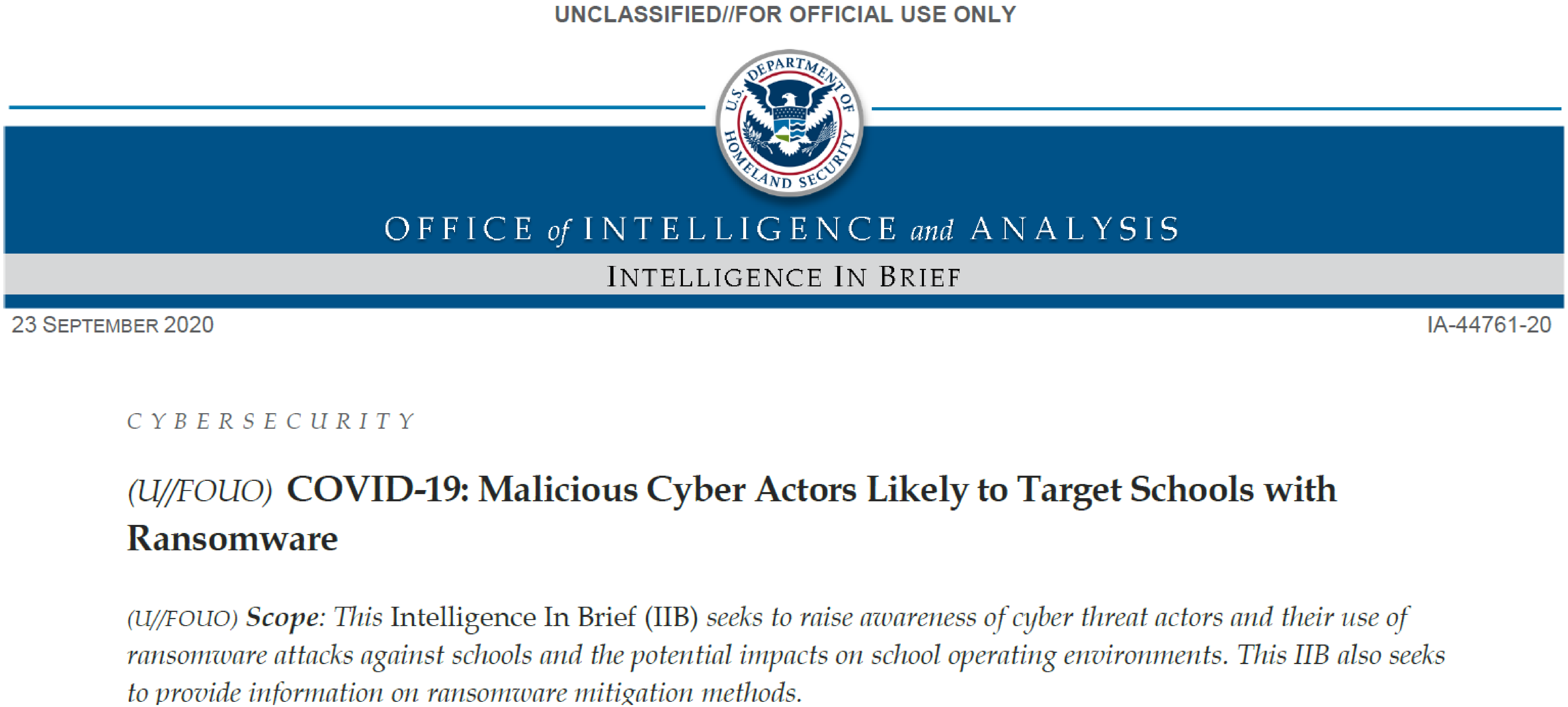
Now national law enforcement leaders are warning about a less obvious threat: the theft of student information.



Faculty, Student Data Compromised in Oregon State Breach

The names and emails of 1,700 Oregon State University students and faculty were exposed after a hacker accessed a computer server. Officials say no Social Security numbers or financial data were exposed in the incident.

US schools have lost 24.5 million records in breaches since 2005



UNCLASSIFIED//FOR OFFICIAL USE ONLY

OFFICE *of* INTELLIGENCE *and* ANALYSIS

INTELLIGENCE IN BRIEF

23 SEPTEMBER 2020

IA-44761-20

CYBERSECURITY

(U//FOUO) COVID-19: Malicious Cyber Actors Likely to Target Schools with Ransomware

(U//FOUO) ***Scope:*** *This* Intelligence In Brief (IIB) *seeks to raise awareness of cyber threat actors and their use of ransomware attacks against schools and the potential impacts on school operating environments. This IIB also seeks to provide information on ransomware mitigation methods.*

WHERE DO WE GO NEXT?

HOW DO WE GET THERE?

Create a robust information security framework with supporting methodologies to generate a comprehensive, highly actionable, and measurable security program and roadmap.

- Robust security requirements gathering across the organization, key stakeholders, customers, regulators, and other parties ensure the security strategy is built in alignment with and supportive of enterprise and IT strategies and plans.
- Security framework that combines COBIT 5, ISO 27000 series, NIST SP 800-53, and CIS critical security controls to ensure all areas of security are considered, covered, and reported upon.
- A comprehensive current state assessment, gap analysis, and initiative generation ensures nothing is left off the table.
- Tested and proven rationalization and prioritization methodologies ensure the strategy you generate is not only the one the organization needs, but also the one the organization will support.

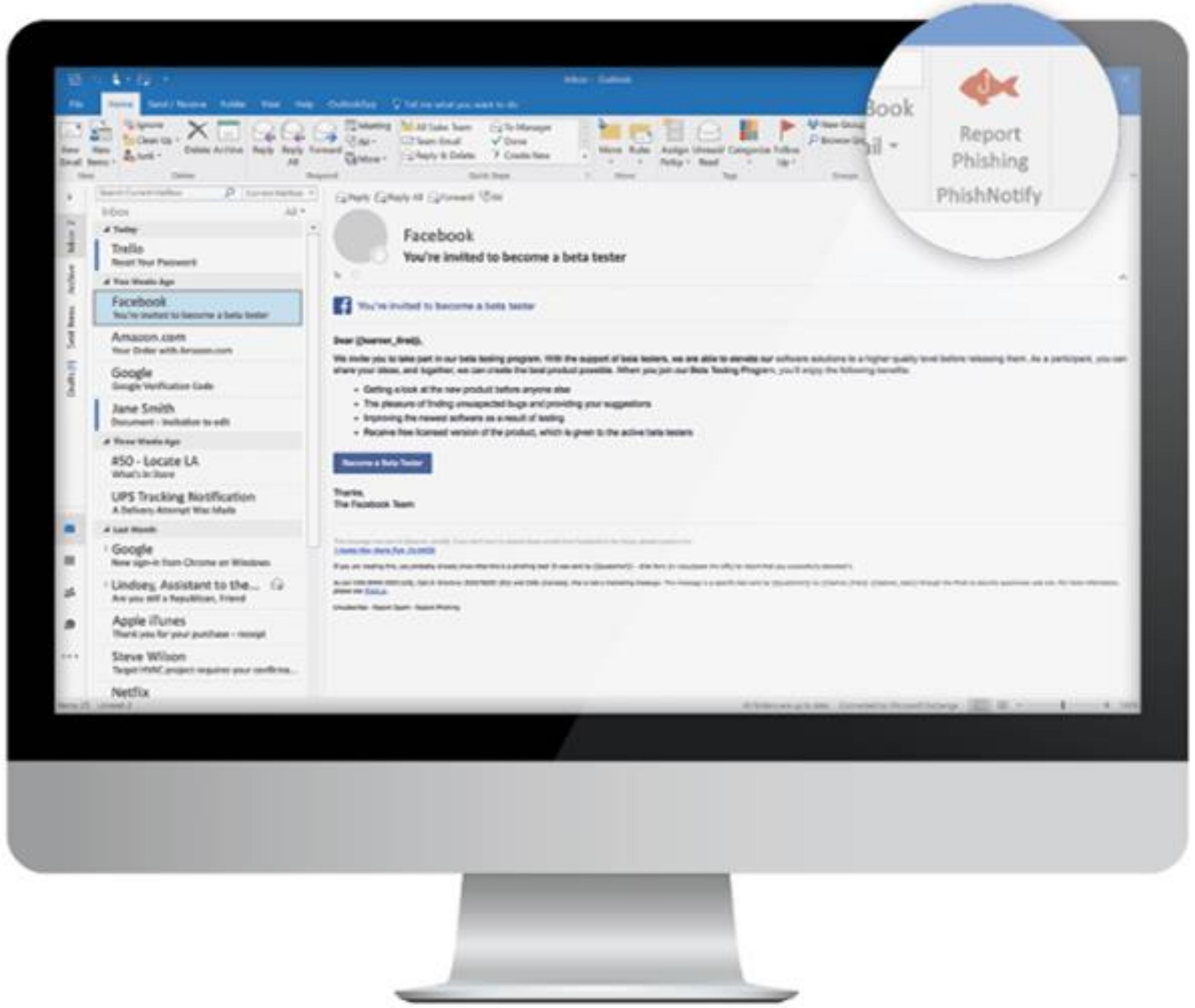
Security Awareness Training

While your employees are your greatest asset…

95% ***of all cyberattacks are caused by*** *human error…*

Companies spend millions on security technology but suffer breaches due to well-meaning employees unaware of security risks.

Phishing Simulator – Report Suspicious Emails


Report
Phishing
PhishNotify
Book
Inbox
Trello
Reset Your Password
Facebook
You're invited to become a beta tester
Amazon.com
Your Order with Amazon.com
Google
Google Verification Code
Jane Smith
Document - Invitation to edit
#50 - Locate LA
What's In Store
UPS Tracking Notification
A Delivery Attempt Was Made
Google
New sign-in from Chrome on Windows
Lindsey, Assistant to the...
Are you still a Republican, Friend
Apple iTunes
Thank you for your purchase - receipt
Steve Wilson
Target HVAC project requires your confirma...
Netflix

Facebook
You're invited to become a beta tester

You're invited to become a beta tester

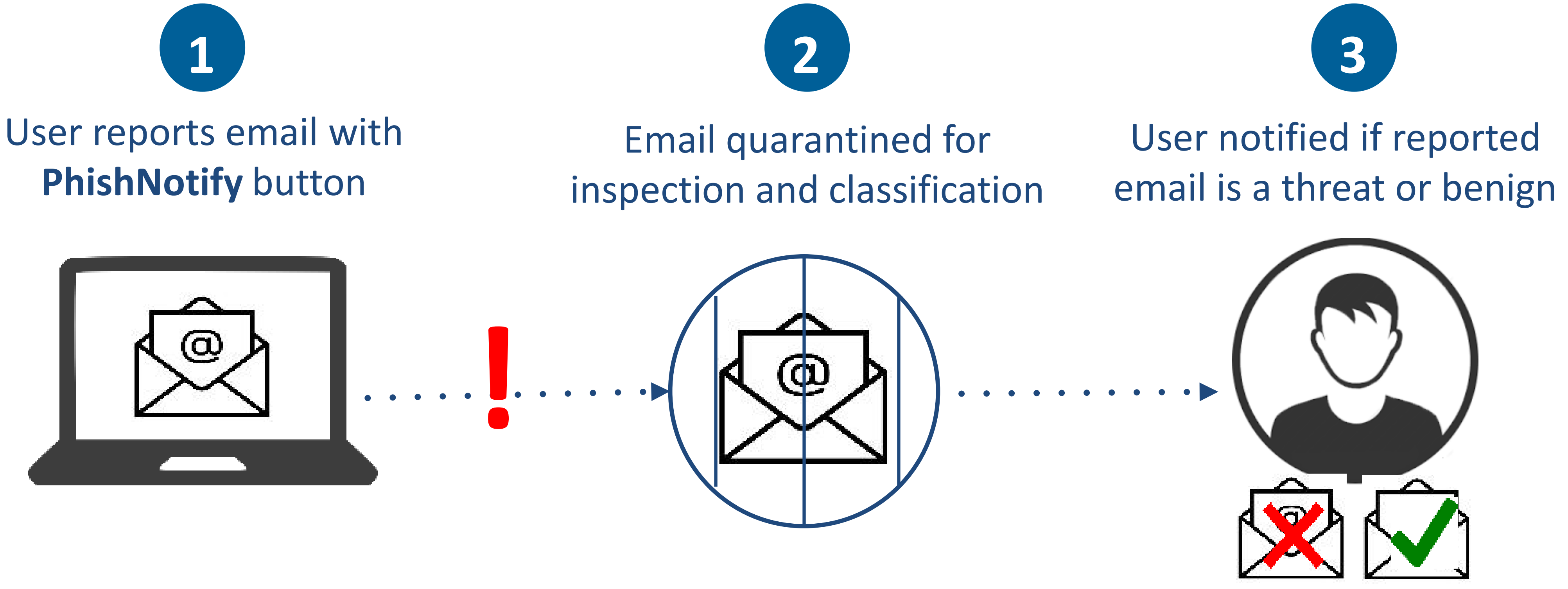
Dear {{learner_first}},

We invite you to take part in our beta testing program. With the support of beta testers, we are able to elevate our software solutions to a higher quality level before releasing them. As a participant, you can share your ideas, and together, we can create the best product possible. When you join our Beta Testing Program, you'll enjoy the following benefits:

- Getting a look at the new product before anyone else
- The pleasure of finding unsuspected bugs and providing your suggestions
- Improving the newest software as a result of testing
- Receive free licensed version of the product, which is given to the active beta testers

Become a Beta Tester

Thanks,
The Facebook Team

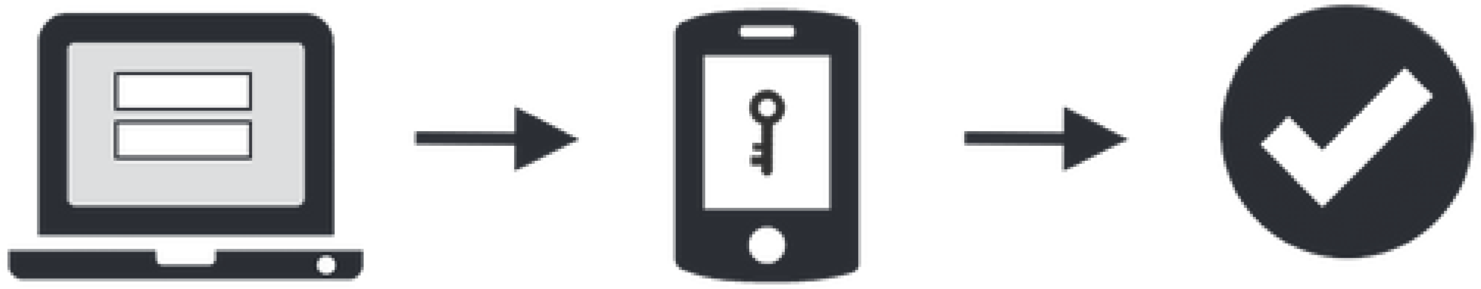


1. User reports email with **PhishNotify** button
2. Email quarantined for inspection and classification
3. User notified if reported email is a threat or benign

What is Two-Factor Authentication?

Two-factor authentication adds a second layer of security to your online accounts. Verifying your identity using a **second factor** (like your phone or other mobile device) prevents anyone but you from logging in, even if they know your password.

How It Works



1. **Enter username and password as usual**
2. **Use your phone to verify your identity**
3. **Securely logged in**

OCTOBER MEANS...

1. HALLOWEEN
2. PUMPKIN SPICE LATTES
3. CYBERSECURITY AWARENESS MONTH

STAYSAFEONLINE.ORG/CYBERSECURITY-AWARENESS-MONTH

Own Your Role in Cybersecurity

- LOCK DOWN YOUR LOGIN
- WHEN IN DOUBT, THROW IT OUT
- KEEP A CLEAN MACHINE
- BACK IT UP
- OWN YOUR ONLINE PRESENCE
- SHARE WITH CARE
- GET SAVVY ABOUT WIFI HOTSPOTS

CYBERSECURITY IS EVERYONE'S JOB.

INCLUDING YOURS.

CYBERSECURITY AWARENESS MONTH

STAYSAFEONLINE.ORG/CYBERSECURITY-AWARENESS-MONTH

Executive summary

Situation

Technology sophistication and business adoption, the proliferation of hacking techniques, and the expansion of hacking motivations from financial to now social, political, or strategic motivations have resulted in organizations facing major security risk. Every organization needs some kind of information security program to protect its systems and assets.

Complication

Performing an accurate assessment of your current security operations and maturity levels can be extremely difficult when you don't know what to assess or how, along with the fact that an assessment alone is only the starting point. Senior management wants to know that adequate targets have been determined and there is a robust plan for how they are going to be met.

Info-Tech **Insight**

1. **Just because you haven't identified a breach doesn't mean you're secure.** A good security program is proactive about closing security gaps because ignorance is never blissful.
2. **Compliance and organizational reputation create an intertwined relationship between the business and your security strategy.** Security programs must be regularly assessed and continuously maintained to ensure security controls align with organizational objectives.

Resolution

Create a robust information security framework with supporting methodologies to generate your organization's comprehensive, highly actionable, and measurable security strategy and roadmap.

- Robust security requirements gathering across the organization, key stakeholders, customers, regulators, and other parties ensure the security strategy is built in alignment with and supportive of enterprise and IT strategies and plans.
- Security framework that combines COBIT 5, ISO 27000 series, NIST SP 800-53, and CIS critical security controls to ensure all areas of security are considered, covered, and reported upon.
- A comprehensive current state assessment, gap analysis, and initiative generation ensures nothing is left off the table.
- Tested and proven rationalization and prioritization methodologies ensure the strategy you generate is not only the one the organization needs, but also the one the organization will support.