

Human Vulnerabilities and Insider Threats

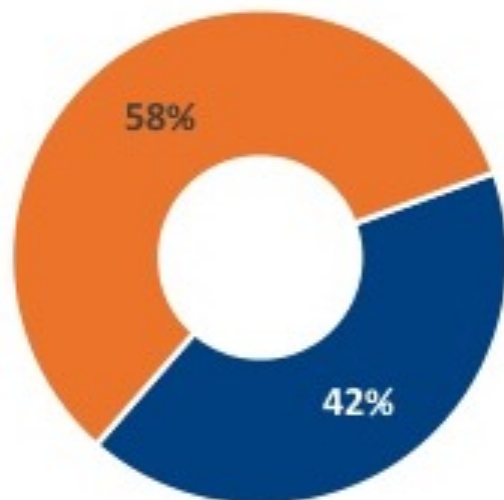
**Sponsored by Empire State Development
Partners: FuzeHub and ISACA**

**Sanjay Goel
University at Albany, School of Business**

Human Vulnerabilities

Security threats

- Humans have become a key impediment to security.
- 58% of security breaches involve humans, and 42% involve technology failures.



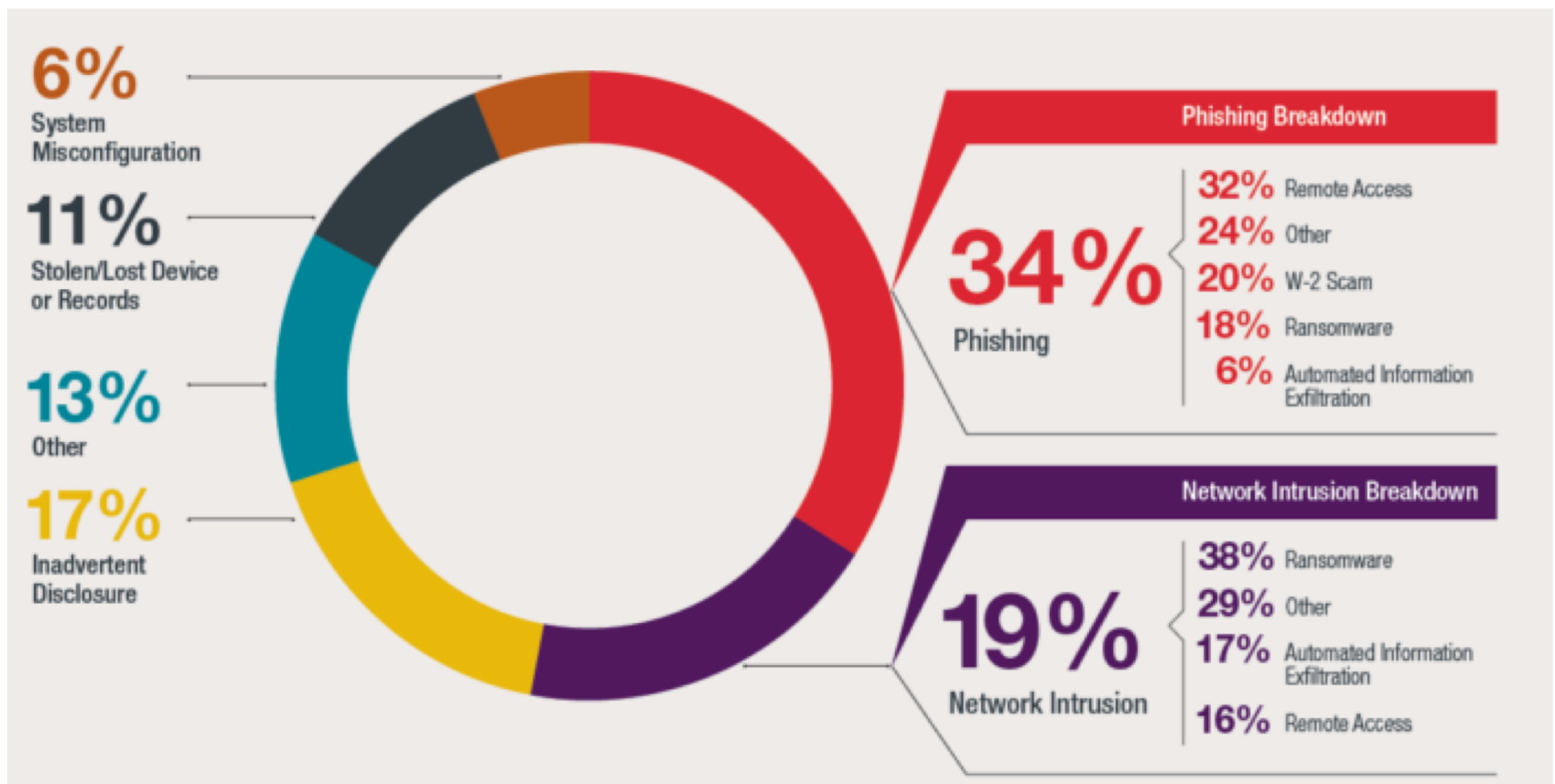
Top Human Error Sources

- 42% General carelessness
- 37% Failure to get up to speed on new threats
- 37% Lack of expertise with websites and applications
- 37% End user failure to follow policies and procedures
- 36% Lack of expertise with networks, servers and other infrastructure
- 34% IT staff failure to follow policies and procedures

Human Vulnerabilities

Breach Statistics

- Humans are central to most types of breaches today.
- Should users be responsible for security decisions despite their poor security record?



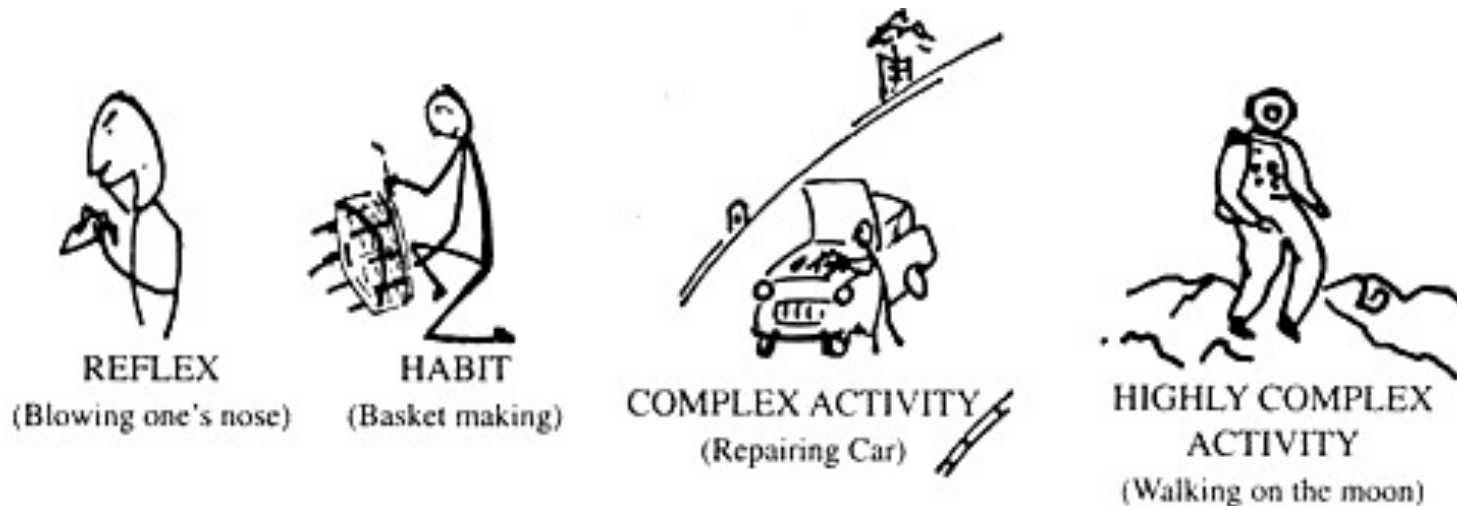
Human Vulnerabilities

Root Cause

- Cognitive Limitations
- Competing Priorities
- Motivation/Apathy
- Personality
- Capability
- Goals

As tasks get more and more complex, fewer and fewer people can accomplish them effectively.

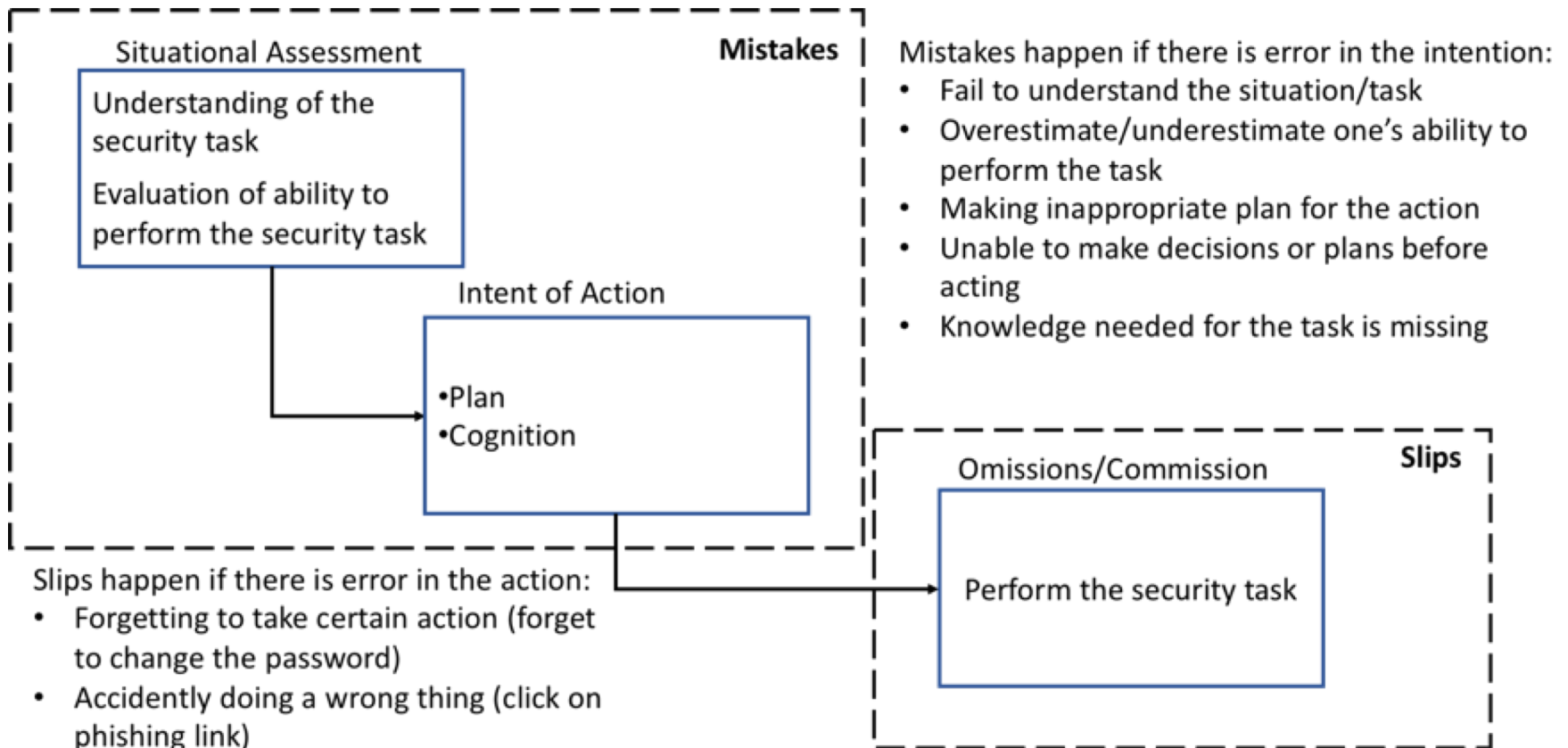
As security gets more complex expect less from users.



Human Vulnerabilities

Human Vulnerabilities

Mistakes and Slips



When under stress (e.g. tight deadlines), people tend to get distracted, and distractions detract from their performance.

Human Vulnerabilities

Cognitive Limitations (Multitasking)

- Employees are constantly juggling multiple tasks , including administrative tasks.
- For security employees, this distraction may lead to errors or mistakes (Distraction Conflict Theory).



http://thumbnails.visually.netdna-cdn.com/TheHighCostofMultitasking_53445af877597_w540.png

Human Vulnerabilities

Competing Priorities

- For employees, productivity is measured through work accomplished.
- Many feel that security processes drain their time and require excessive effort.
- Employees struggle to balance security and productivity.
- When under pressure, some may focus on the primary task and ignore secondary tasks, such as security compliance.

End user restrictions
disrupt work and create
productivity barriers

81%

of CISOs say users see security
as a barrier to innovation

74%

of CISOs said end users
have expressed frustration

572 hours

spent annually by help desks
on user requests for access

<https://www.bromium.com/cybersecurity-vs-productivity-the-cisos-dilemma/>

Human Vulnerabilities

Motivation

Amotivation

Extrinsic Motivation


Intrinsic Motivation

*External
regulation*

Introjection

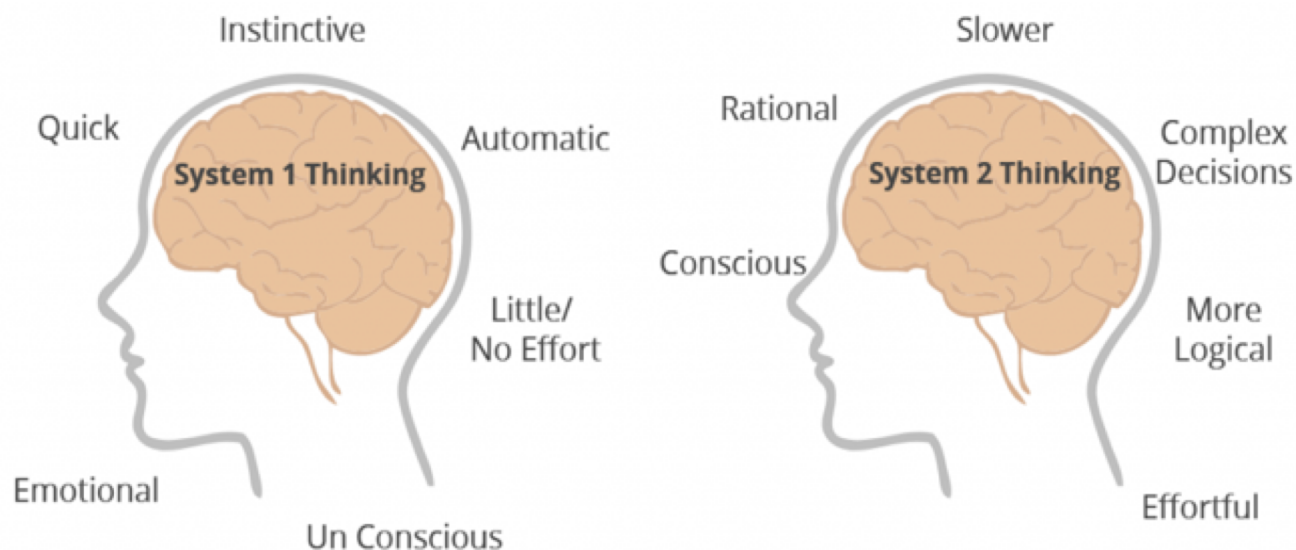
Identification

Integration

- 
- Human motivation exists on a scale of intrinsic to extrinsic.
 - When people are intrinsically motivated, they perform the task on their own (e.g. raising children, taking vacations, etc.).
 - Security is a cumbersome task, providing little/no intrinsic motivation.
 - Lack of intrinsic motivation necessitates extrinsic motivation.
 - e.g. threats, punishments, sanctions, rewards, and incentives

Human Vulnerabilities

Decision Analysis



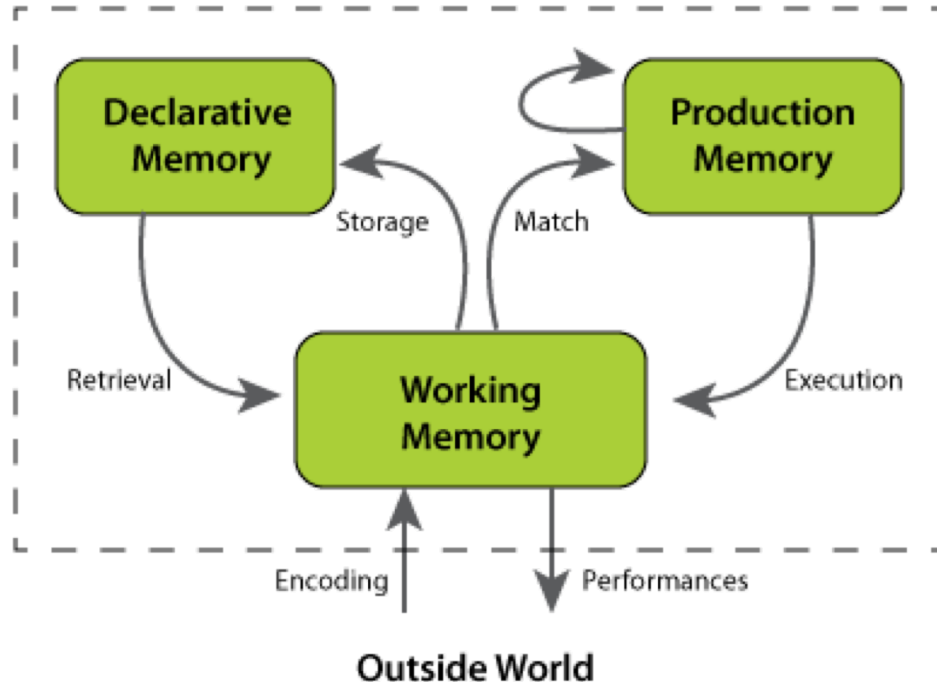
- System 1 thinking is quick and automatic, while system 2 thinking is deliberate and conscious.
- Most training pushes people towards system 2 thinking.
- About 95% of peoples' decision making is in system 1 thinking.
- Phishing takes advantage of system 1 thinking by giving users familiar contexts.

Weak Passwords

Passwords

Cognitive Limitation

- People show better memory performance for the basic meaning, rather than the details, of past events.
- Retrieving a password requires knowledge about its source (the system in which one should use a particular password), and its structure (the precise organization of letters, numbers, and symbols that compose the password).
- Recommendations for creating secure passwords require users to retrieve memories for detailed (verbatim) information, which fade quickly over time, and are subject to interference.

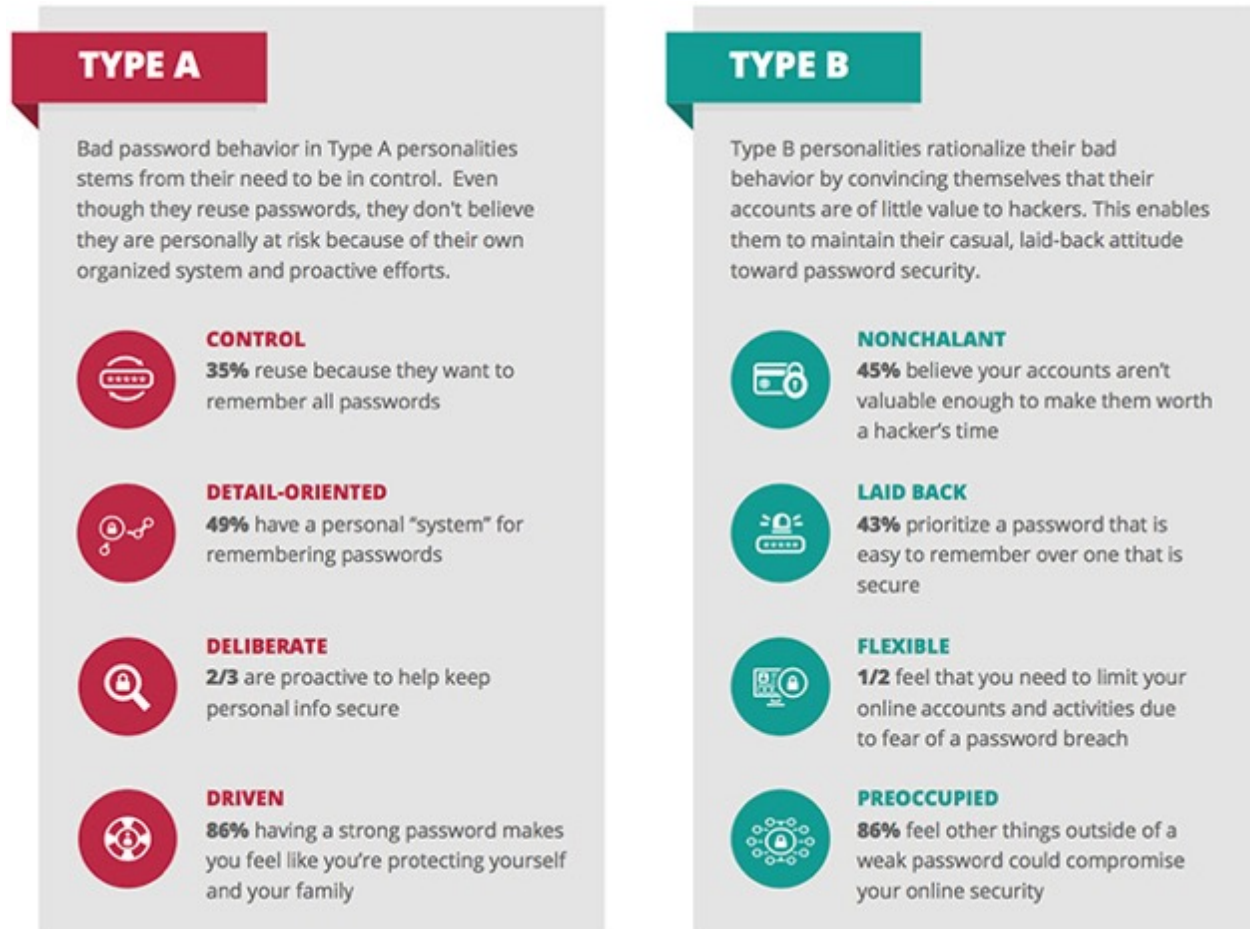


Older adults often show a general decline in memory, especially in tasks involving recall

Passwords

Poor Password Practices

- Passwords of personal significance
- Short passwords
- Excessively simple passwords
- Reusing passwords
- Writing down passwords



<https://www.helpnetsecurity.com/2016/09/29/risky-password-practices/>

Passwords

Complex Password Rules

- No Dictionary Words, Proper Nouns, or Foreign Words
- No Personal Information
- Length, Width and Depth
 - uppercase letters e.g. A, B, C
 - lowercase letters e.g. a, b, c
 - numerals e.g. 1, 2, 3
 - special characters e.g. \$, ?, &
 - alt characters e.g. μ, £, Æ
- At least 8 characters long
- Use different passwords for different accounts

HINTS

Take a sentence and turn it into a password.

Select an image of an interesting place (Mount Rushmore). Select a photo of a familiar or famous person (Beyonce). Imagine some random action, along with a random object (Beyonce driving a Jello mold to Mount Rushmore).

Come up with 12 random words to create a password phrase (and password).

Get a password vault.

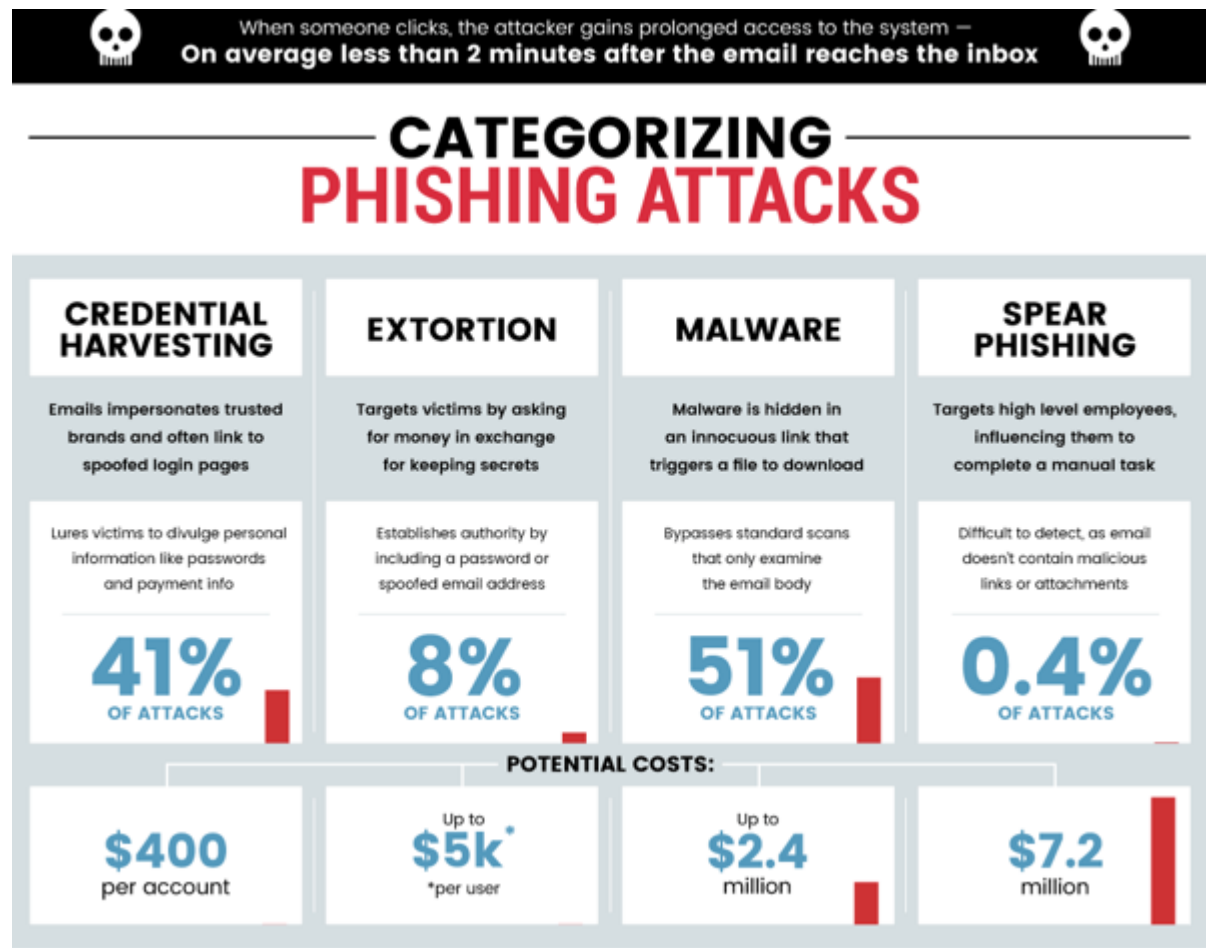
Phishing

Phishing

Scope

- 83% of people get phishing attacks.
- 76% of businesses get phishing attacks.
- 1 in 100 emails is a phishing email.
- 95% of attacks on enterprise networks are the result of a successful spear phishing.
- 38% of successful phishing attacks result in compromised accounts.

<https://www.stanfieldit.com/wp-content/uploads/Phishing-Statistics.png>

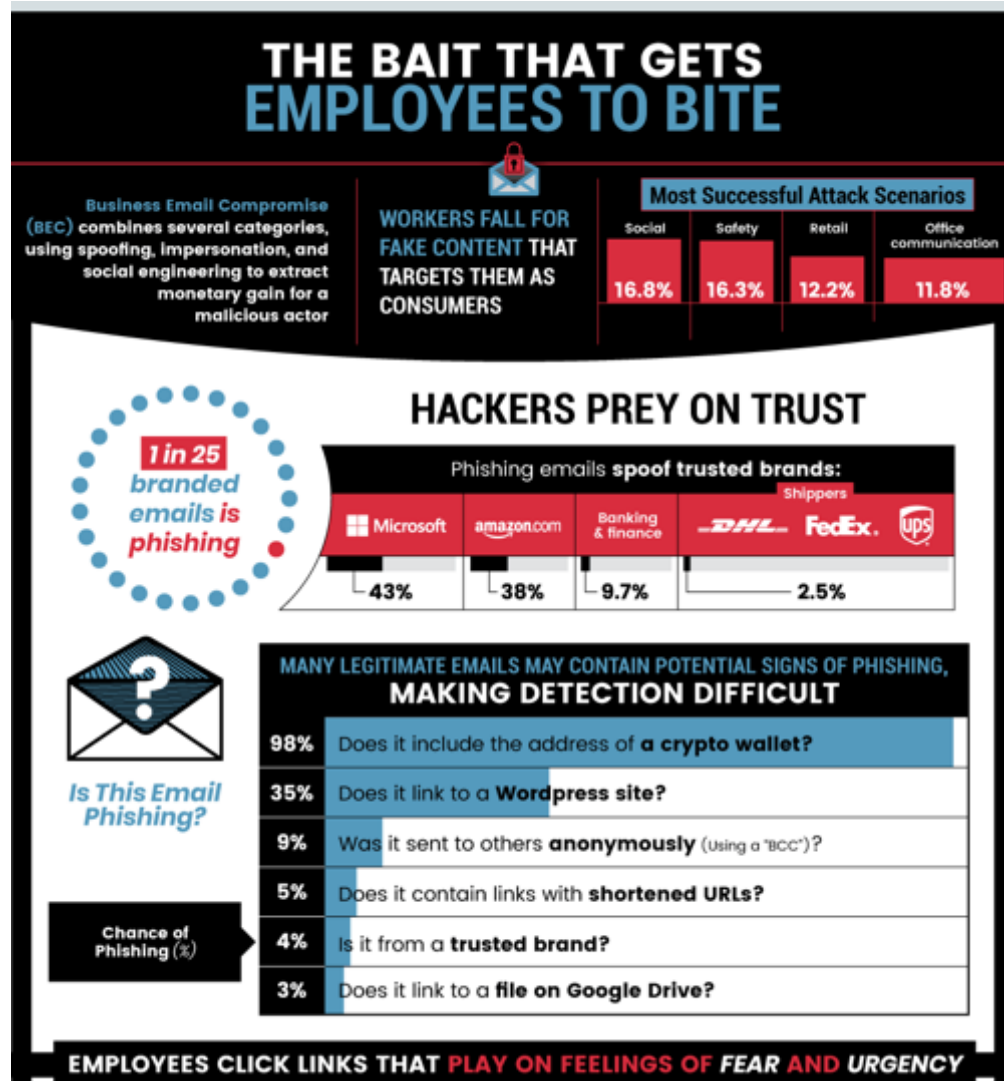


<https://smallbiztrends.com/2019/07/phishing-statistics.html>

Phishing

Psychological Manipulation

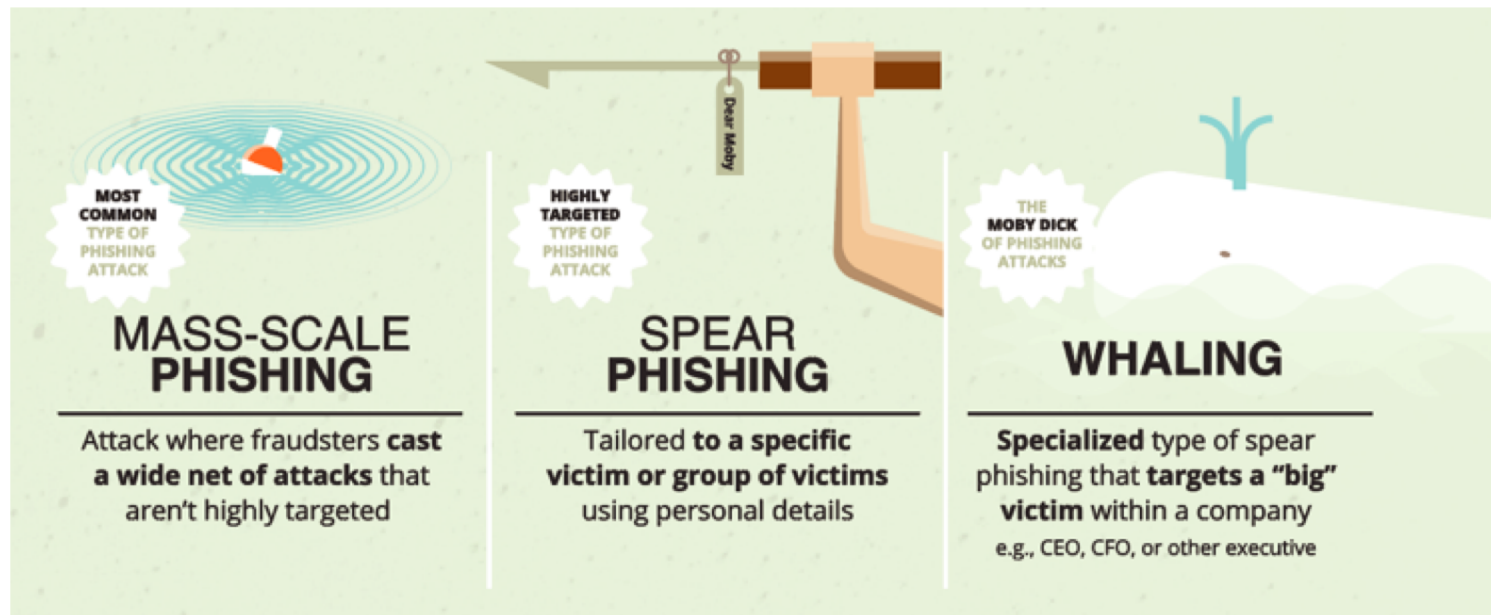
- Personality traits (e.g. trusting)
- Autonomous mode of operation
- Perceived invincibility
- Lack of knowledge
- Stress/Workload



Phishing

Contextualization

- Contextualization based on situational cues (student courses) and individual factors (family members) results in increased susceptibility.
- Persuasion techniques include rewards (e.g. gift cards), urgency (e.g. loss of opportunity), social outcomes (LinkedIn invite), fear (IRS audit), and social causes, etc.

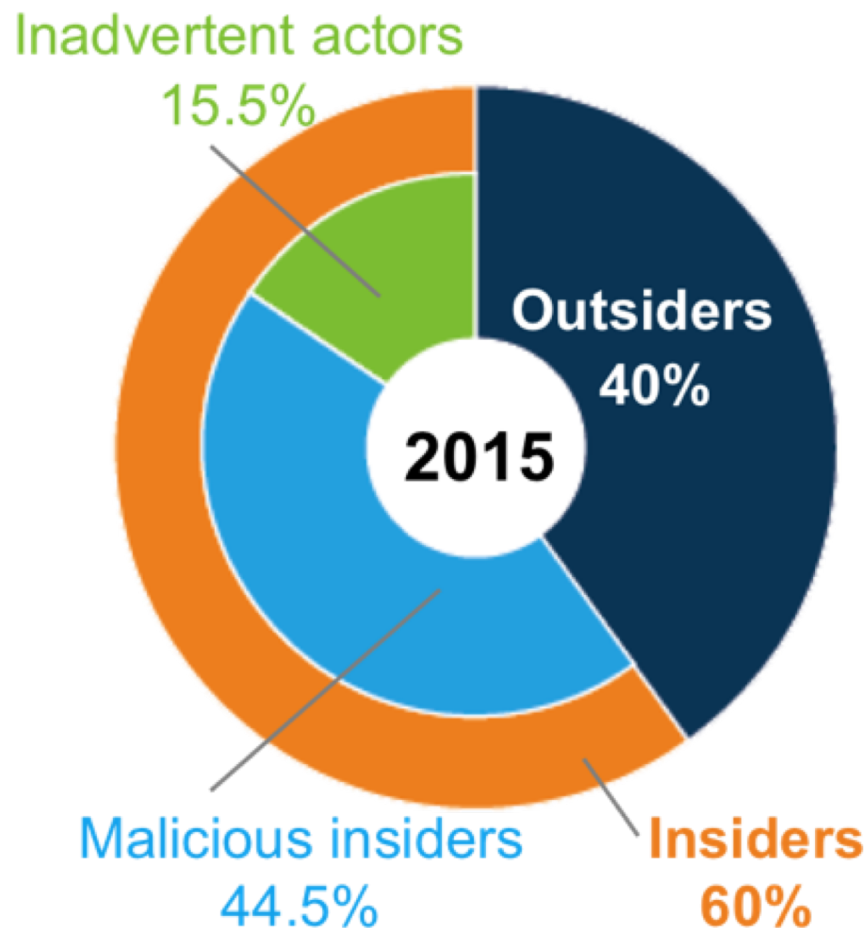


Malicious Insider Threats

Insider Threats

Losses

- The Verizon 2019 Data Breach report says that 34% of all breaches in 2018 were caused by insiders.
- The Ponemon Institute 2018 Cost of Insider Threats study shows that the average cost of an insider-related incident is around \$513,000 (up 15% from 2018), and that a company needs on average 197 days to identify a breach and 69 days to contain it.



Malicious Insiders

Risk

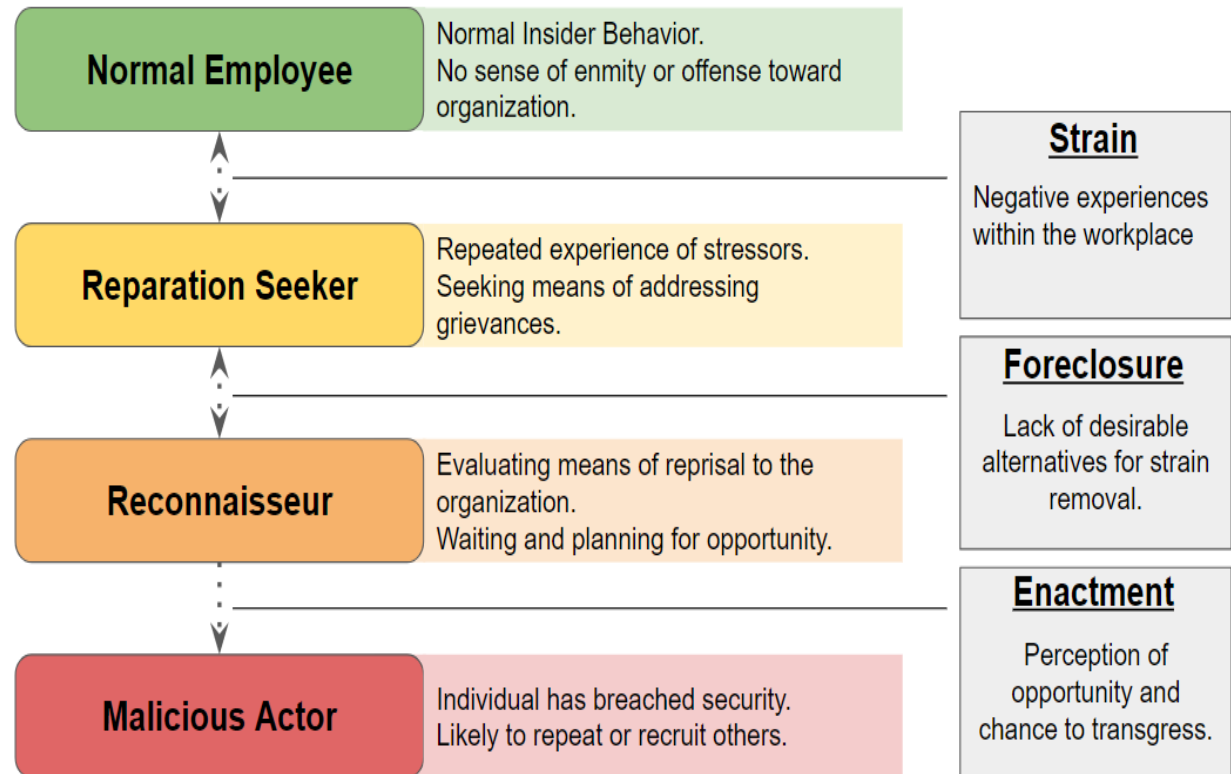
- Insiders pose a significant risk due to the damage they can cause through either malicious or inadvertent actions.
- Privileged users can perform essentially any operation on critical systems, and users often have accumulated more entitlements than they need for their current job role.
- Malicious insiders can be disgruntled employees, mercenaries, or just greedy, i.e. acting for financial benefit.
- Exploited insiders may be “tricked” by external parties into providing data or passwords they shouldn’t.
- Careless insiders may simply press the wrong key, and accidentally cause critical data loss.



Malicious Insiders

Mechanism

- ‘Normal’ employees can turn ‘malicious’ during their employment.
- There are several reasons for malicious behavior, including greed, social justice, personal injustice, patriotism, etc.



Malicious Insiders

Greed (Examples)

Anthony Levandowski, a lead engineer at Waymo, Google's self-driving car project, left in 2016 to found Otto, a startup that developed self-driving trucks. Otto was acquired by Uber, and Levandowski was put in charge of Uber's self-driving department. His wasn't a sudden move, but a thoroughly planned set of actions. Waymo alleges he downloaded 9.7 GB of their highly confidential files, trade secrets, blueprints, design files and testing documentation before he left.

<https://www.ekransystem.com/en/blog/real-life-examples-insider-threat-caused-breaches>

An employee of AMSC, Dejan Karabasevic stole his employer's trade secrets and sold them to the Chinese company Sinovel for \$20,000. He was also promised a 6-year \$1.7 million contract. Karabasevic was the head of the automation engineering department at AMSC, and often made business trips to China. He accepted an offer from Sinovel to download the source code of turbine software from an AMSC computer. Sinovel used the software on turbines ordered for US companies, and the software copy was detected.

Malicious Insiders

Civic Duty (Examples)

Ana Belen Montes was a military analyst for the DIA who spied on behalf of the Cuban government for over 16 years. Montes was a leading and well-respected expert on U.S. policy towards Cuba, and was a true ideologue in the sense that she sold secrets not for money or personal disgruntlement, but because she was fighting what she saw as “the good fight” against unfair perceived U.S. policy towards Cuba.

Edward Joseph Snowden is an American whistleblower who copied and leaked classified information from NSA in 2013 when he was a CIA employee and subcontractor. He revealed NSA surveillance programs and the Five Eyes Intelligence Alliance with the cooperation of telecommunication companies and European governments.

Snowden claims to have committed these acts out of civic duty and patriotism, believing the public has the right to know about the abuses he saw reflected in the classified documents he had access to.

Malicious Insiders

Patriotism

Greg Chung spied for China while being employed at Rockwell and later Boeing, stealing hundreds of boxes worth of documents pertaining to the military and spacecraft from 1979 to 2006, when he was finally caught.

Walter Liew, 59, of Orinda, was convicted in 2014 of 10 felony charges of economic espionage, theft of trade secrets, obstruction of justice and tampering with a witness and with evidence, and he was sentenced to 15 years in prison and a \$28 million fine. He sold DuPont technology pertaining to the production of a valuable white pigment to China.

What to do?

What are we doing?

Current Response (Constrain)

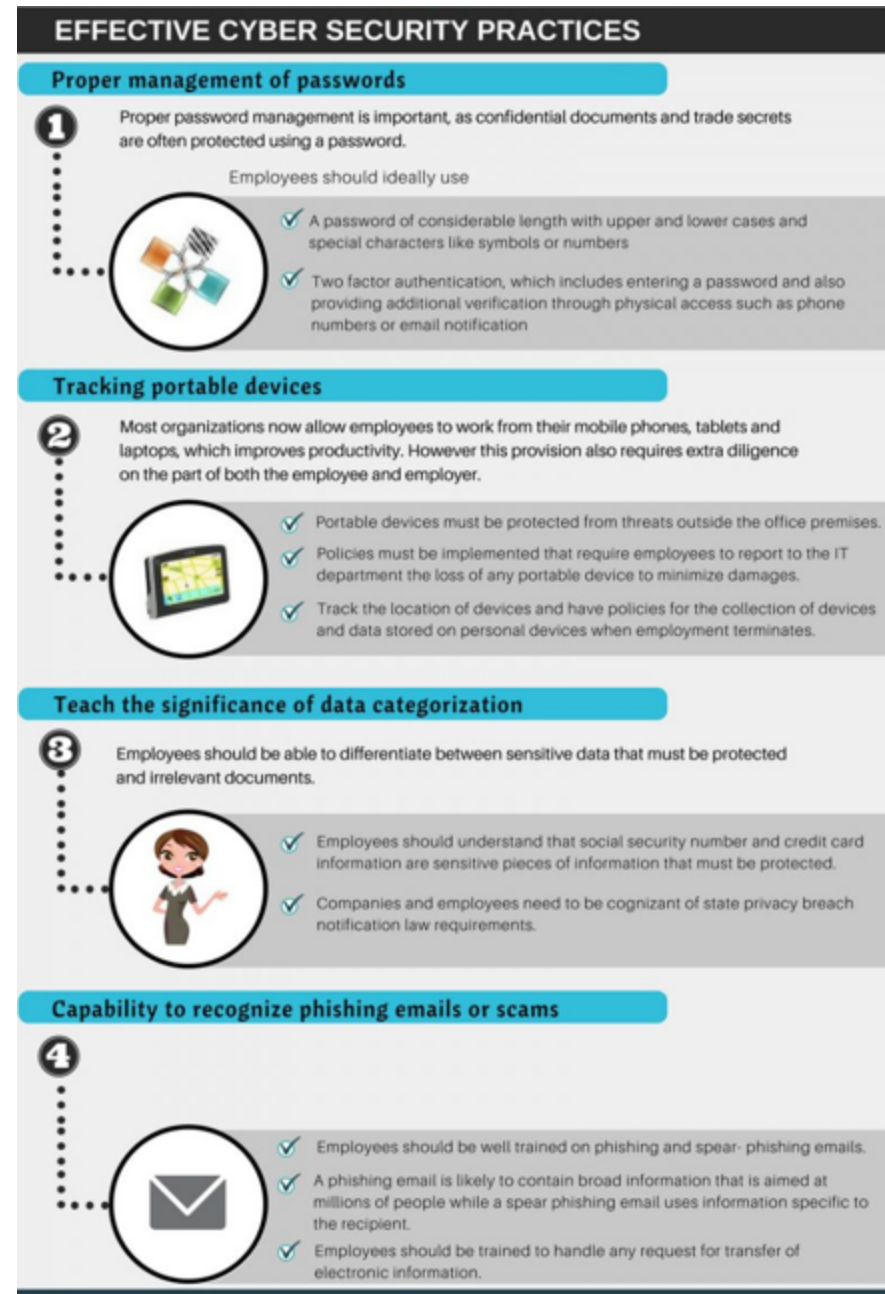
- Developing restrictive security policies
- Restricting access to external websites
- Restricting access to external software
- Restricting traffic: whitelisting (ports, ip addresses, etc.), blacklisting (ip-addresses)
- Controlling the perimeter
- Taking links away from emails
- Leads to ... loss of productivity, stifling of innovation, employee discontent, finding new ways of avoiding restrictions



What are we doing?

Current Response (Train)

- Personnel are trained on their assigned information security-related duties and responsibilities.
- Key topics: risks associated with individual roles, policies, standards, and procedures, reporting potential indicators of insider threat.
- Challenges in training:
 - Lack of motivation
 - Conflict with productivity
 - Constantly changing environment
- The Result
 - Frustrated employees
 - Training expenditures



What are we doing?

Current Response (Threaten)

Current approach, policies, fear appeals, threats, and sanctions to motivate users

While there are some people who feel motivated by fear, others are paralyzed by it. “The problem is, negative emotions often breed other negative emotions,” - Stephanie Creary

“Fear may appear at first to be a mechanism that helps people stay alert to the unacceptability of failure, but it can ironically be a source of failure instead.” –Andrew Carton

<https://knowledge.wharton.upenn.edu/article/fear-motivate-workers-make-things-worse/>

University at Albany, School of Business
Center for Information Forensics and Assurance

Psychological Contract



<https://www.businessballs.com/building-relationships/the-psychological-contract/>

What are we doing?

Security Fatigue

- This cycle of constrain, train, and threaten has left users feeling overwhelmed and frustrated.
- In a NIST study more than half of the respondents reported feeling “overwhelmed and bombarded, and they got tired of being on constant alert, adopting safe behavior, and trying to understand the nuances of online security issues.”



<https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly>
<https://dilbert.com/strip/2005-09-10>

What should we do?

Assume incidents will occur (Analytics)

- Switch from protection to detection: detect rapidly evolving threats, responding to intrusions quickly, monitoring insider threats.
- Set up a log management system (operating system, application, security logs).
- Add data analytics to provide a unified view of an enterprise—both a real-time and an historic view of events.
- Establish an incident-management capability that includes preparation, detection, reporting, analysis, containment, and recovery.



Source: <https://nyia.org/publications/guiding-principles/>

What should we do?

Change Password Protection

- Enforce password standards: complex, no-reuse for multiple generations, one-time temp passwords, and store/ transmit passwords encrypted.
- Authenticate users prior to access; use replay-resistant authentication; prevent reuse of passwords, disable access after defined period of inactivity.
- Enforce multifactor authentication for network access to all accounts, and local access to privileged accounts.
- Multifactor authentication: (1) something you know (e.g., password); (2) something you have (e.g., token generator, smartphone); something you are (e.g., fingerprint or iris scan).

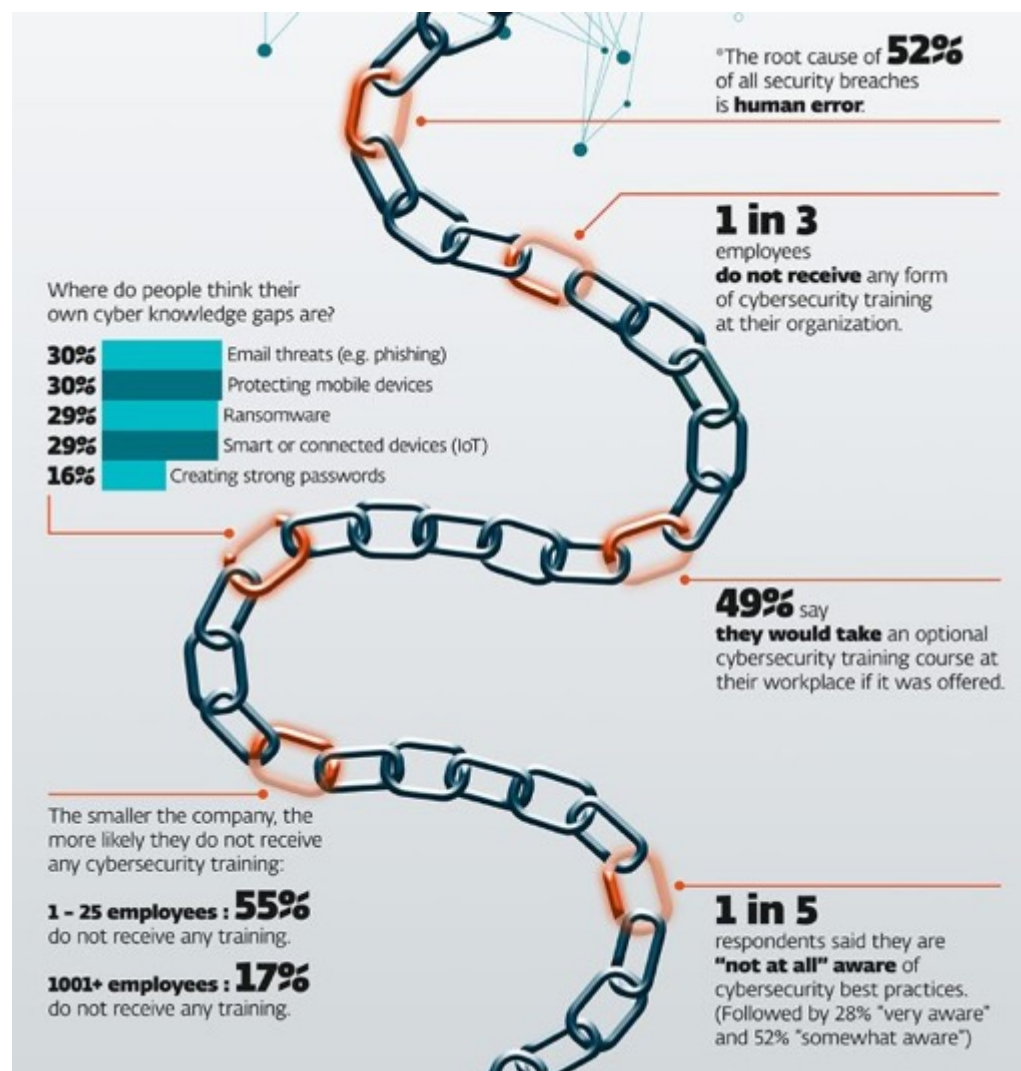


Source: <https://nyia.org/publications/guiding-principles/>

What are we doing?

Adaptive Training

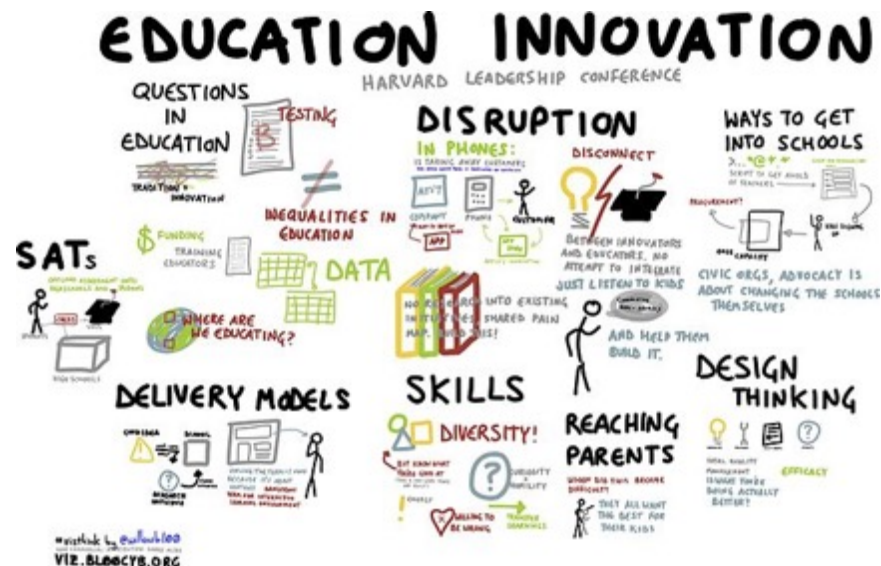
- Over-training can lead to security fatigue.
- Understand the knowledge gaps and provide focused training in gap areas.
- Engage employees in assessing training needs.
- Use adaptive training that shifts based on user responses
- Make training engaging, rather than information and policy heavy



What should we do?

Education Innovation (Workforce)

- Cybersecurity degree programs are proliferating, but with a large range in quality.
- CAE—the government’s response (DHS/NSA) to accrediting best programs.
- Education needs to reflect the reality that while breaches are inevitable, detection and response are critical.
- Humans are a weak link in security - need interdisciplinary security focus.
- Some feel that the reason we were caught off guard with Russian interference in the elections, and with 9/11, was a “failure of the imagination.” This is a critical point, that speaks to the need to bring more people, and more diversity (of gender, nationality, experience) into the field.

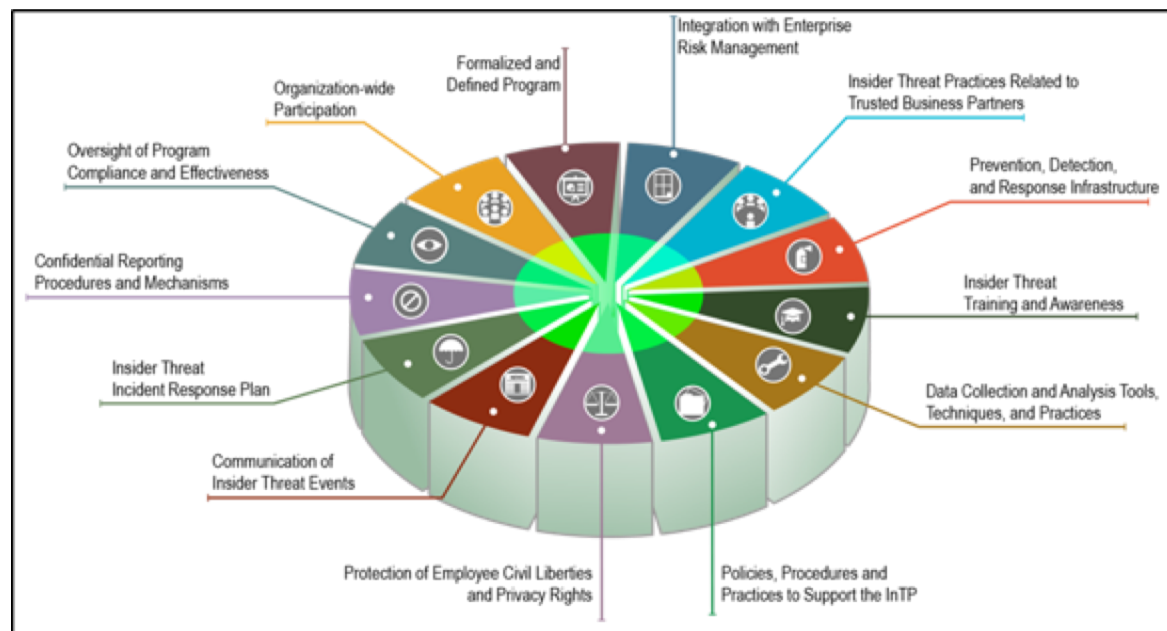


<http://coriolisinnovation.com/index.php/services/education-innovation/>

What should we do?

Insider Threats (Monitoring)

- Create a comprehensive insider threat mitigation plan
- Put program in place to continuously monitor internal networks and systems
- Limit access on as-needed basis for different employees
- Put policies in place for actions against insiders
- Screen employees while hiring, and maintain high job satisfaction for employees



<https://insights.sei.cmu.edu/insider-threat/2017/04/formalized-insider-threat-program-part-2-of-20-cert-best-practices-to-mitigate-insider-threats-series.html>

What should we do?

insider Threats (Active Indicators)

- Intentional behavior can be conceptualized as function of motivation (incentive), capability, opportunity.
- Through use of active probes we can form predictive profiles using personality and other measures to identify threats.
- Environmental and disposition precursors may involve greed, perception of being undervalued, disgruntlement, perceived social injustice, patriotism.
- We designed scenarios to build situational context and tested user behavior on simulated opportunities to steal data.

Scenario: Social Injustice

Joe works for a large conglomerate that produces water filtration systems that are critical for poor countries where the water supply is severely contaminated. Typical water filtration systems are very expensive, however, Joe and his colleagues have developed a system that is highly cost effective. Despite the cost of producing this new filtration system being only a few dollars, Joe's company has gauged the price to charge hundreds of dollars. Ultimately, Joe is outraged at this policy, since many countries will no longer be able to afford this system, leading to widespread sickness and death.

Conclusions

Conclusion

Managing Human Vulnerabilities

- The 'constrain, train and threaten' approach causing security fatigue.
- Security restrictions are killing productivity and innovation.
- Understand human cognition, motivation, and decision making in understanding security risks.
- Reduce the security burden on users (multi-factor authentication, artificial intelligence, and analytics).
- Security is a complex task that requires users to be motivated and trained using creative approaches.



<https://www.securitymagazine.com/articles/90319-artificial-intelligence-is-fundamental-to-the-future-of-cybersecurity-smes-say>