BPM

Top Cybersecurity Threats Facing Nonprofits

David Trepp

October 28, 2021

David Trepp
Partner, CyberSecurity Assessment Services

- US Army Veteran
- MS Physical Chemistry
- Serial Tech Entrepreneur
- Personal Interests
  - Rock Climbing
  - Bicycle Touring
  - Information Science
    - Thermodynamics

dtrepp@bpmcpa.com

BPM

Information Security Expertise

- BPM CyberSecurity Assessment (CSAS) personnel ***are not*** experts at planning, building, or managing information security controls
  - We are not here to endorse or sell any solutions

- BPM CSAS personnel ***are*** experts at compromising information security controls
  - We are ethical hackers who've performed thousands of penetration tests

- This introductory presentation will provide an **ethical hacker's perspective** on the current cybersecurity threat landscape

Questions and comments are encouraged

BPM

Table of Contents

BPM

Overview of the Threat Landscape

Threat Sources

Hacktivists	Monkeywrenching	Digital Vigilante Justice • Anonymous • Islamic Jihad
Foreign Nation-State Sponsored Entities	Espionage Time Bombs Extortion / Reprisal, *e.g.* Sony	Physical Damage • 2008 - Stuxnet destroyed Iranian uranium enrichment centrifuges with malware that may have been delivered via USB key • 2014 - German Steel Mill blast furnace meltdown and "massive damage" due to malware delivered via phishing email
Criminal Profiteers	Identity Fraud Credit Fraud Tax Return Fraud Medical Fraud • Post-mortem Medicare • Elective Surgery • Prescription • Record Tampering	Cryptocurrency Mining Corporate Fraud • Extortion, *e.g.* Ransomware • Account Takeover • Purchase Order • Real Estate Escrow • Intellectual Property Theft • Insider Trading • ACH / Check Transactions
Employees, Vendors & Contractors	Untrained Negligent	Disgruntled Malicious

BPM

Hacktivists

Republican Governors Association Targeted in Exchange Attacks

Breach Notification Report Reveals Some PII Could Have Been Exposed

Scott Ferguson (Ferguson_Writes) • September 16, 2021

Anonymous says it will release massive trove of secrets from far-right web host

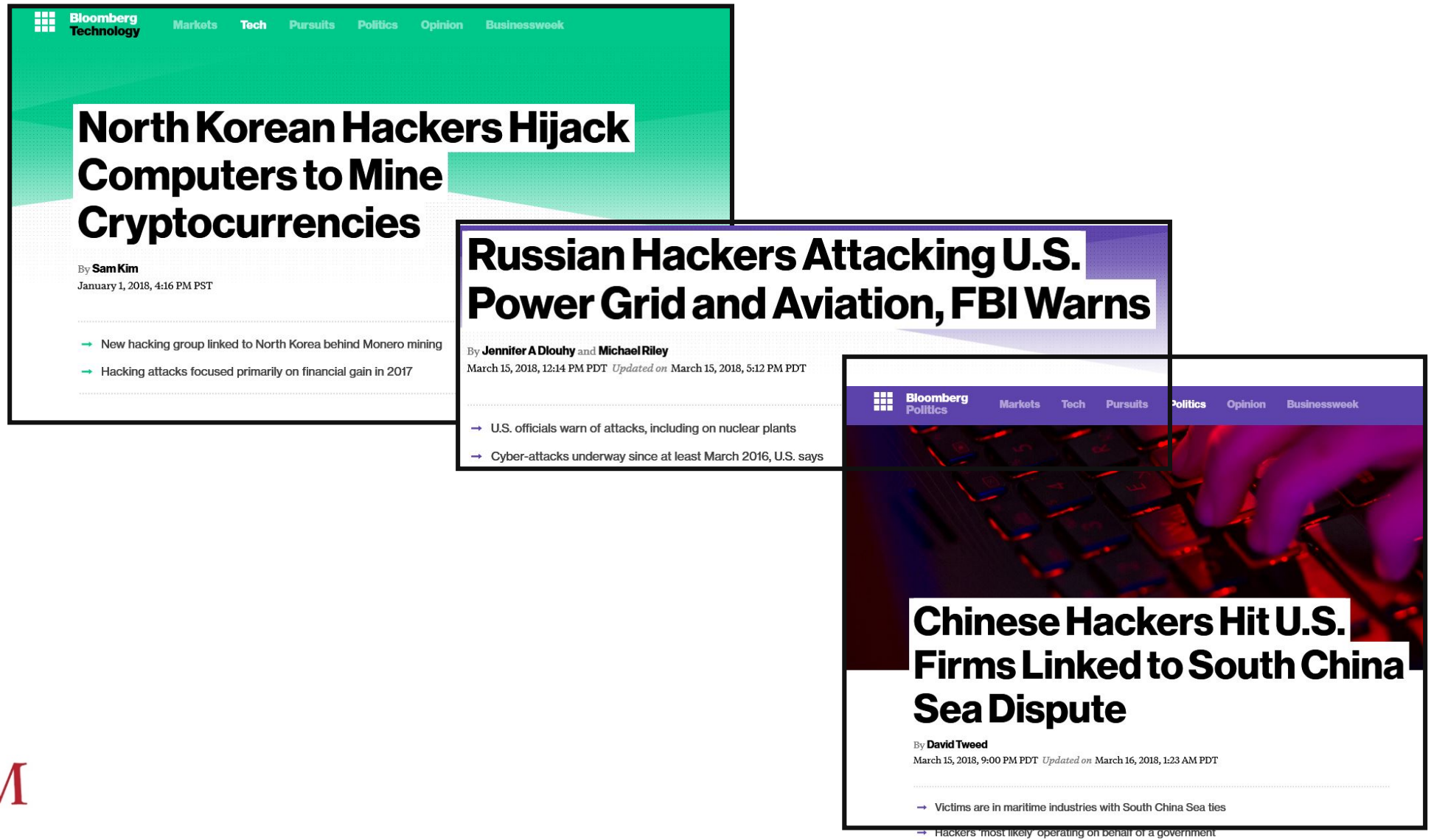
Move follows hack inspired by Texas abortion ban.

Claire Goforth Tech Published Sep 14, 2021 Updated Sep 18, 2021, 9:43 am CDT

Politically motivated hacks often focus on releasing embarrassing information into the public domain

BPM

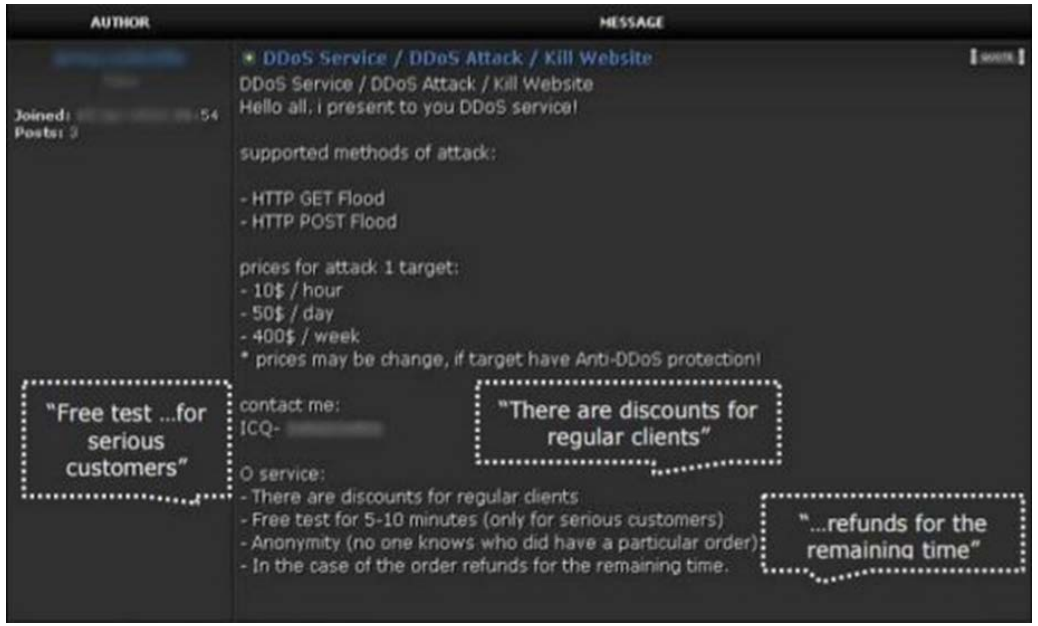
Nation State Threat Sources



BPM

Cyber Crime Pays

Attack kits for sale on the dark web:
elite hacking skills not required



Negotiating with a dark web seller: note test options, repeat customer discounts & refunds for unused services

Hacked Instagram Accounts in Bulk	1,000 - 10,000 accounts $15 - $60
Botnet: Blow-Bot Banking Botnet	Monthly Basic Rental $750 | Monthly Full Rental $1,200 | Monthly Support $150
Disdain Exploit Kit	Day $80, Week $500, Month $1,400
Stegano Exploit Kit: Chrome , FireFox, Internet Explorer, Opera, Edge	Unlimited Traffic, Day $2,000 Unlimited Traffic, Month $15,000
Microsoft Office Exploit Builder	Lite exploit builder $650 Full Version $1,000
WordPress Exploit	$100
Password Stealer	$50
Android Malware Loader	$1,500
Western Union Hacking Bug For World Wide Transfer	$300
DDoS Attacks	Week long attack $500 - $1,200
ATM Skimmers: Wincor, Slimm, NCR, Diebold	$700 - $1,500
Hacking Tutorials	Multiple Tutorials $5 - $50

Cost of hacking tools and services on some underground cybercrime forums (Source: Armor)

BPM

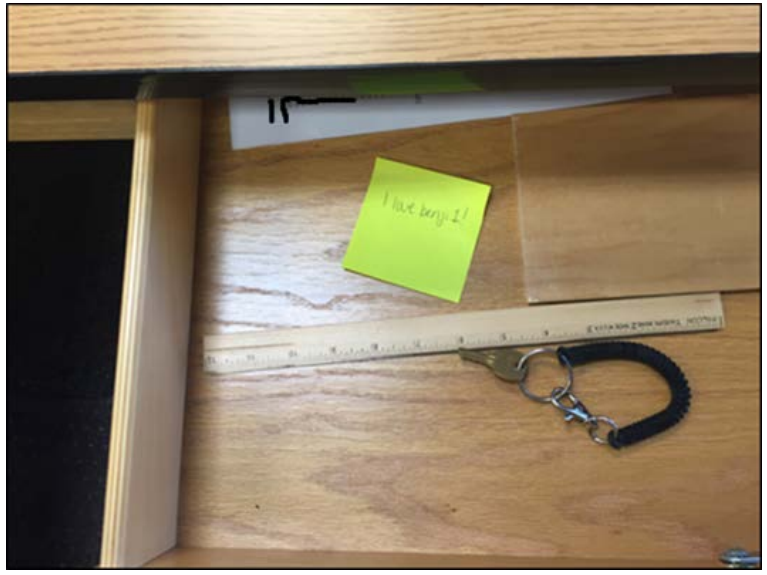
WARNING: Visit the Dark Web at Your Own Risk!

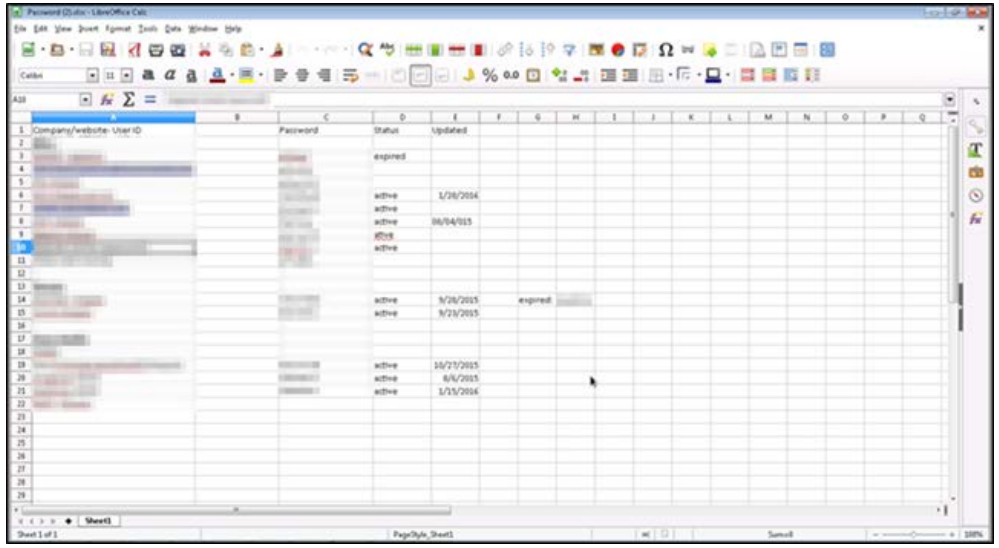
Malicious and/or Negligent Insiders

S.F. officials locked out of computer network

SAN FRANCISCO Engineer jailed after allegedly refusing to hand over password

By Jaxon Van Derbeken Published 4:00 am PDT, Tuesday, July 15, 2008





BPM

Three Primary Attack Vectors

- Human

- Physical

- Technical

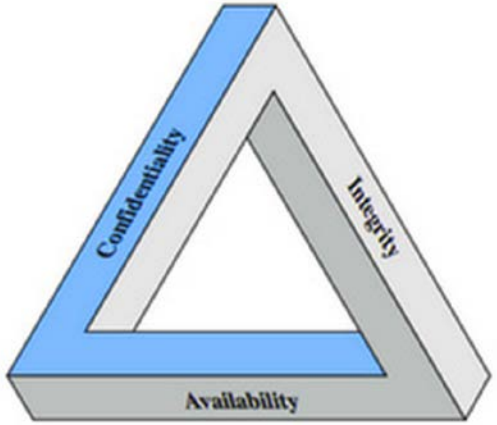
Alone *and* Combined

BPM

Infosec Concepts: Risk Assessment

Risk: A *measure* of the extent to which an organization is threatened by a potential circumstance or event (threat); a function of impact and likelihood

Risk = Likelihood * Impact



What is the likelihood of a threat agent exploiting a threat?

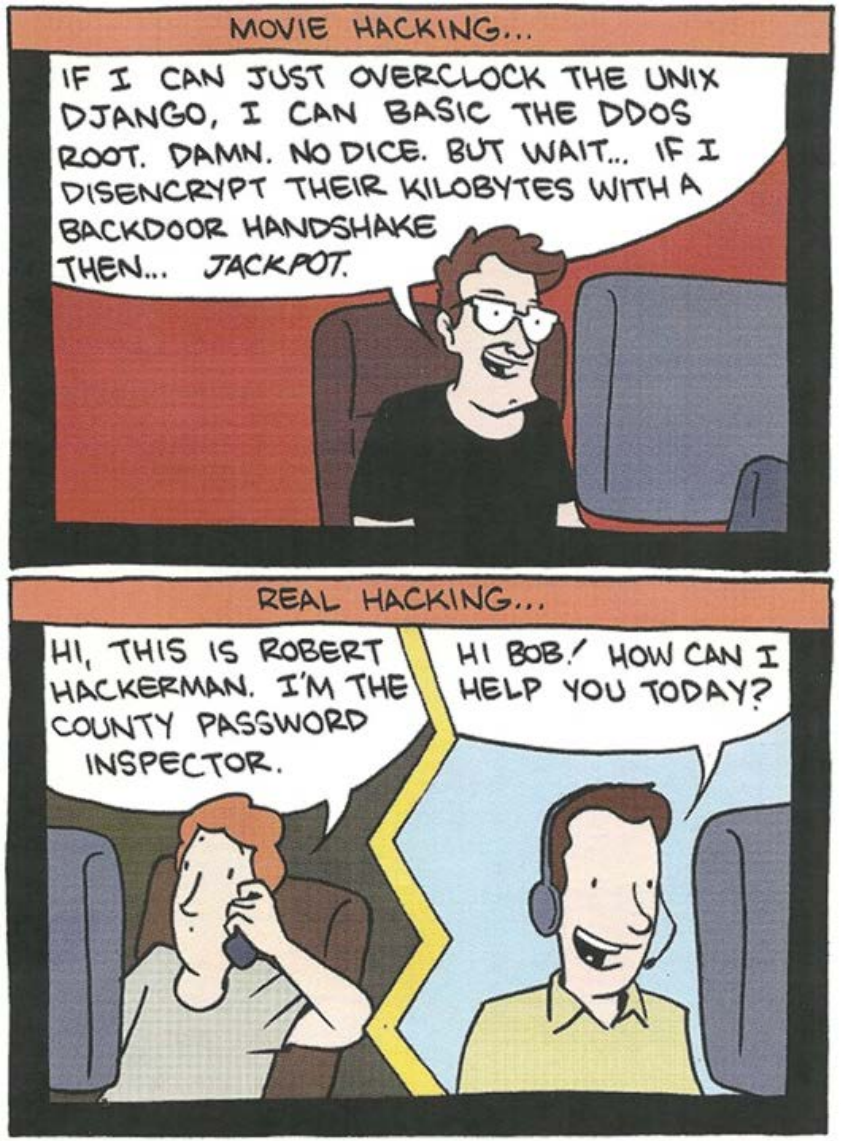
- High Likelihood: Facing the Internet, Technically easy to defeat
- Low Likelihood: Hidden within network, Technically challenging

What is the impact of a successful exploit?

- Low Impact: Inconvenience
- High Impact: Disruption of service, Disclosure of sensitive customer information, and/ or fraudulent transaction

See NIST Special Publication 800-30, Guide for Conducting Risk Assessments

Why Is Social Engineering So Likely To Succeed?



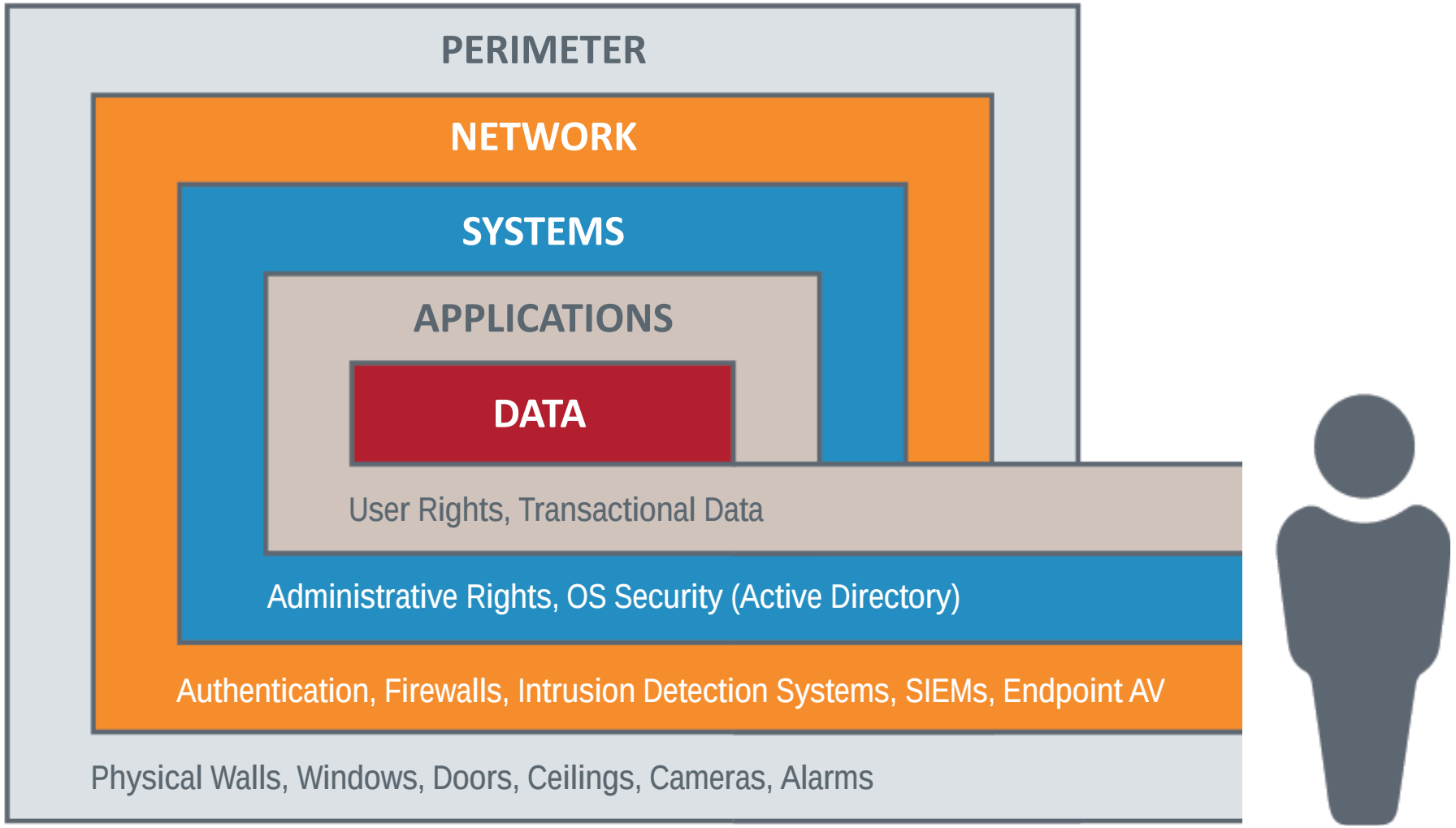
- Societies couldn't exist without an innate "assumption of truth"
- Human cognitive abilities generally decline when faced with unusual circumstances

Statistics suggest the average employee fails four social engineering attacks before becoming "inoculated"

Source:
Saturday Morning Breakfast Cereal
www.smbc-comics.com

BPM

Why Is Social Engineering So High Impact?



BPM

Worsening Threat Landscape

- Evolving Social Engineering Techniques
  - Headline Opportunism, *e.g.* Pandemic
- Releases of sophisticated, formerly secret hacker's tools into the public domain are rampant, and lead to common ransomware and related attacks
  - Equation Group
  - Hacking Team
- Boundaries are blurred between systems with different responsible parties
- The 'Internet of Things' continues to increase the Internet's attack surface area
- Newly documented vulnerabilities are being released at a dizzying rate
- Software vendor supply chain related vulnerabilities

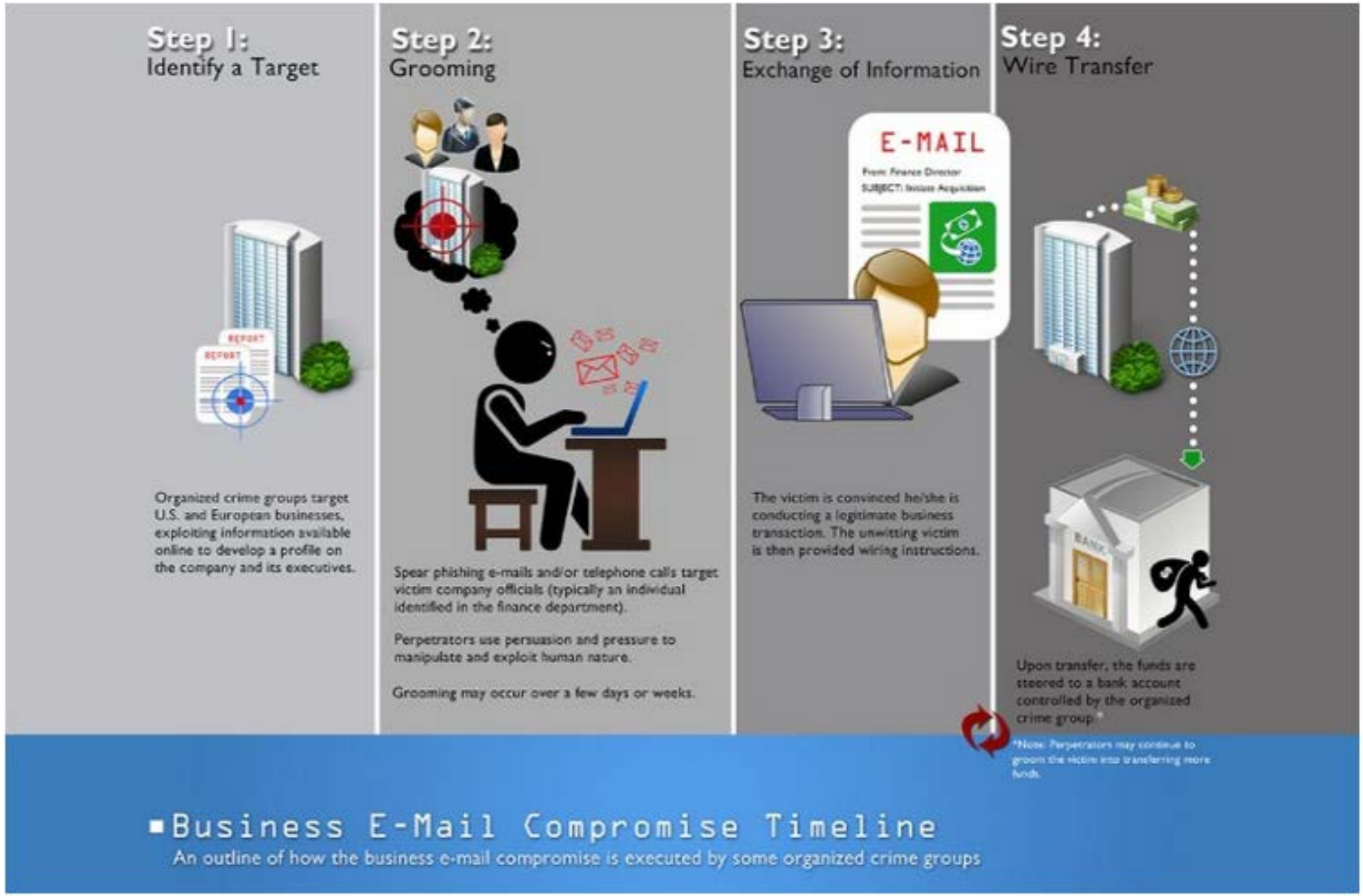
Threat Scenario I: Payables Fraud – Fictitious Vendor Scenario

Payables Fraud - Fictitious Vendor Scenario

- Targets accounts payable personnel
  - Change of vendor payables address or bank routing
  - Urgent payment/expense
- Most commonly occurs via email…
  - Perform Prior Reconnaissance
    - ID target with accounts payable responsibilities
      - LinkedIn, Facebook, Instagram, etc.
    - Name dropping
  - Probe Email for Weaknesses
    - Address spoofing
    - Attachment and link controls
  - Attack
    - Groom
    - Pressure
    - & Close
- …or via phone

  same recon & attack modes as above, plus
  - Caller ID spoofing
  - Even Artificial Intelligence-aided voice “deep-fakes”

BPM



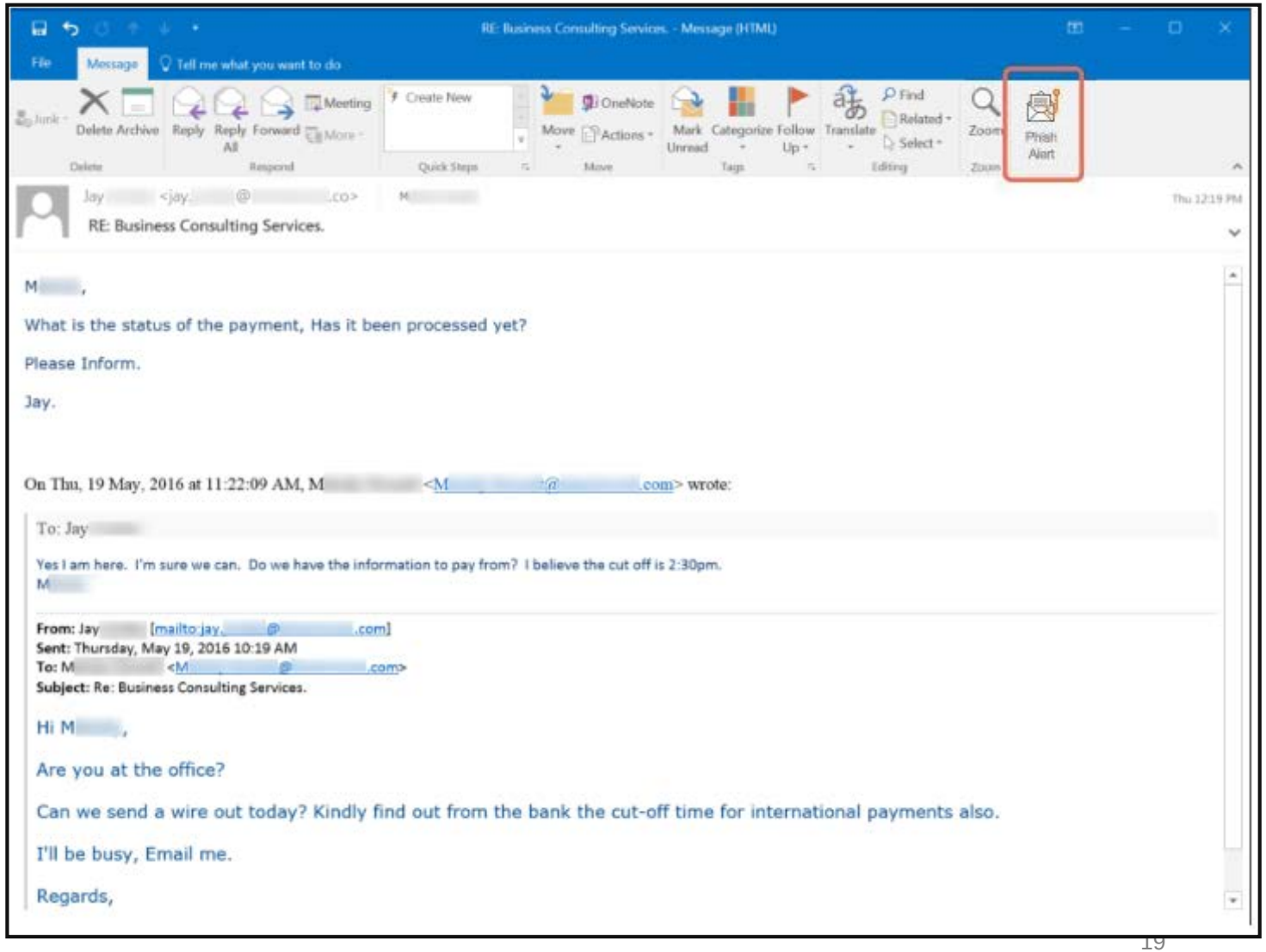
Business email compromise attack timeline (Image source: FBI)

CEO Impersonation email

Recent Fictitious Vendor breach investigation

-Over 20 emails were exchanged between attacker and victim

- -Reconnaissance & initial hack
  - -Learn all the players
    - -Target Accounts Payable employee
  - -Executive email account takeover
    - - via password breach
- -Grooming via
  - -email spoofing
  - -Executive impersonation
- -Flattery
  - -"we know we can rely on you…"
- -Persuasion
  - -"time is short"
- -Pressure & Close the deal!



BPM

Email Technical Risk Management Controls

- Email Platform Configuration
  - Implement 2FA/MFA
  - Prohibit MX gateway bypass
  - Disable/restrict EWS access
  - Prohibit enumeration
- Inbound email Controls
  - Filter Attachments & URLs
    - Gateway
    - Email client
    - End point
  - Prohibit Spoofing
    - Valid domains & subdomains
    - Alternate domains
    - Invalid domains
  - Rate Limit
- Prohibit macros in document and spreadsheet files
- Outbound email
  - Data Loss Prevention

BPM

Fictitious Vendor Email Risk Management

Train Users

- Always confirm sender - hit “reply” to see if return address matches (alleged) sender
- Do not open suspicious attachments
- Hover over links, and verify destination URL, before clicking
- Never enter credentials on a foreign site – without an explicit IT directive
  - Whenever in doubt, check with IT first!

Fictitious Vendor Phone Risk Management

Train Users

- Verify the purpose of the call
  - Have a prepared denial response
- Verify the phone number
  - Caller ID check via dial-back
- No payables changes should be executed or changed without internal (2nd party) approvals
  - Outbound call to known-good phone #

Threat Scenario II: Ransomware

Ransomware: A Cyber Pandemic

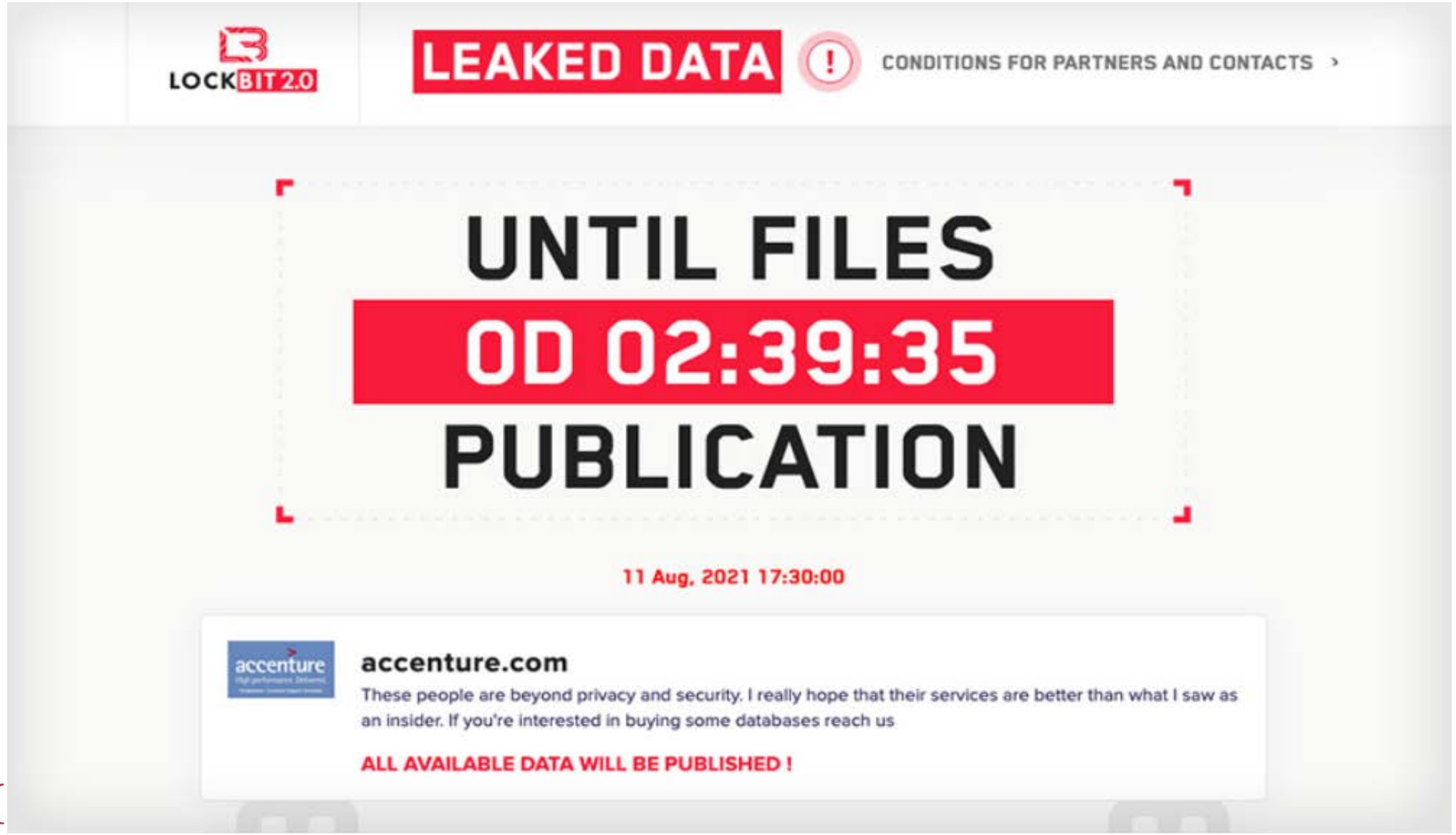
- Often delivered via email attachment/link
  - May lure users to malicious web destination
  - May include malicious attachment
- Sometimes performed via the phone
  - Lure users to malicious web destination
- Sometimes via app/code download sites
  - Masquerading as legitimate application or patch/update for legit app
- And also via document portals
  - Misc. file upload services
    - HR resumes
    - Other application portals
  - Box, Dropbox, et al

Ransomware: A Cyber Pandemic

- High-Profile Examples
  - CNA Insurance - Top 10 Insurance Firm
    - Fake Browser “update” delivered via legitimate site
    - Paid $40 million
  - Colonial Pipeline - Houston-NY petroleum transport
    - Paid $4.4million, but much of it returned by FBI
  - Accenture - Large professional services organization
    - Declined to pay
      - Sensitive client data stolen and posted
- Smaller organizations don’t make headlines

BPM

Ransomware: A Cyber Pandemic



BPM

Prepare to Respond to Ransomware

Do they likely have our sensitive data?
How long can we afford to be down?
How quickly can we restore from bare metal?

- Fight
  - Removal Software
    - AVG, Trend Micro, BitDefender, Kaspersky, et al
  - Decryption Keys
    - FBI REvil key
    - Trustwave Blackbyte key
  - Offline Backups
    - Air-Gapped – physically disconnected from network after backup
    - Cloud/Hosted – logically disconnected, hardened authentication
- Pay
  - Have a cryptocurrency wallet set up
    - No guarantees
    - Legal gray area

BPM

Configure A Breach Laptop

- Disconnected From Network
- System Administration Tools
  - System/Domain Administrator Privilege Levels
  - Wireshark
  - Microsoft SysInternals
- Password Database(s)
  - All critical systems and applications
- Backup/Restore Software
- Critical Application License Keys
- Key Contact Info
  - Internal staff
  - IT & security vendors
  - Legal counsel & law enforcement
- Ransomware Eradication Tools & Decryption Keys

Threat Scenario III:
Work From Home Exploits

Common Remote Work Vulnerabilities

- Increased organizational attack surface
- Consumer-grade network infrastructure
- BYOD equipment
- Local storage
- Physical security
- Email and chat to perform communications previously performed in person
- Web meetings
  - Increased third party dependencies, *e.g.* web conference apps
  - Insecure meeting information distribution
  - Insecure meeting credentials
- Distractions & social engineering
  - Work and personal computing intermingled
  - Work-from-home scripts
  - Pandemic scripts

BPM

A Few Telework Security Controls

- Understand & enforce your organization's telework policies & procedures
- Control authentication
  - Dual-factor
  - Use long, difficult to guess passwords
  - Encrypt credential storage
- Ensure smart home devices, *e.g.* virtual assistants, smart TVs, *etc.*, are not activated when discussing sensitive information
  - "Texas" & "Lexus" sound a lot like "Alexa"
  - "Seriously" sounds a lot like "Siri"
- Enhance endpoint protections
  - Anti-virus/anti-malware
  - Browser controls, *e.g.* script prohibitions
- Issue organization-owned hardware
  - Encrypt all end-user hard drives
    - Turn computers off evenings/weekends
  - Lock (Win + L) computers when taking a break
- Secure web meetings
  - Passphrases
  - Waiting rooms
  - Don't email all meeting information, use out-of-band method (text, call, or chat) to deliver meeting information
- Make sure home networks are configured securely
  - Change default passwords on ISP routers/modems, and patch them
  - Make sure home WiFi is not using WEP or WPA1/WPA2 – use WPA3
- Use a VPN/Cloud applications for communications with office systems
  - Secure logins with multi-factor authentication
  - Single Sign-On improves convenience

A Few Mobile Device Security Safeguards

- Be an aware mobile device user
  - Practice safe application storefront protocols
  - Be cognizant of QR code dangers
  - Inspect all links before clicking
  - Consider banning mobile phones from sensitive conversations
    - Use a specialized camera/mic cover
- Limit mobile device malware attacks
  - Keep O/S & browser current via updates/patches
  - Anti-virus/malware
- Apply the concept of “Least Privilege”
  - Does your phone need to do everything your laptop does?
- Apply session controls
  - Logout when done
- Apply the concept of “Least Functionality” to mobile devices
  - Turn off location services, bluetooth, personal hotspot, & WiFi when not in use
  - Do not use public WiFi if not fully trusted (stick to the LTE network, when feasible)

BPM

Threat Scenario IV: Vendor Supply-Chain Exploits

Many Breaches That Make Headlines

Occur after the system or application already exists via one, or a combination of, the following techniques:

- Social Engineering
  - Use email, text, chat, phone, snail mail, and/or in-person interactions to get employees to do and/or reveal things they shouldn't
- Credential Compromise
  - Find, intercept, guess, crack, bypass, spoof, and/or request credentials
- Patch Exploit
  - Exploit vulnerabilities on systems missing critical patches
- Misconfiguration Breach
  - Take advantage of weak configurations, often vendor default configurations
- Boundary Incursion
  - Trespass across interconnected system boundaries, typically from a less-secure system to a more-secure one
- Code Logic Abuse
  - Direct information gathering, session hijacking, scripting, injection, and/or privilege escalation attacks against application logic

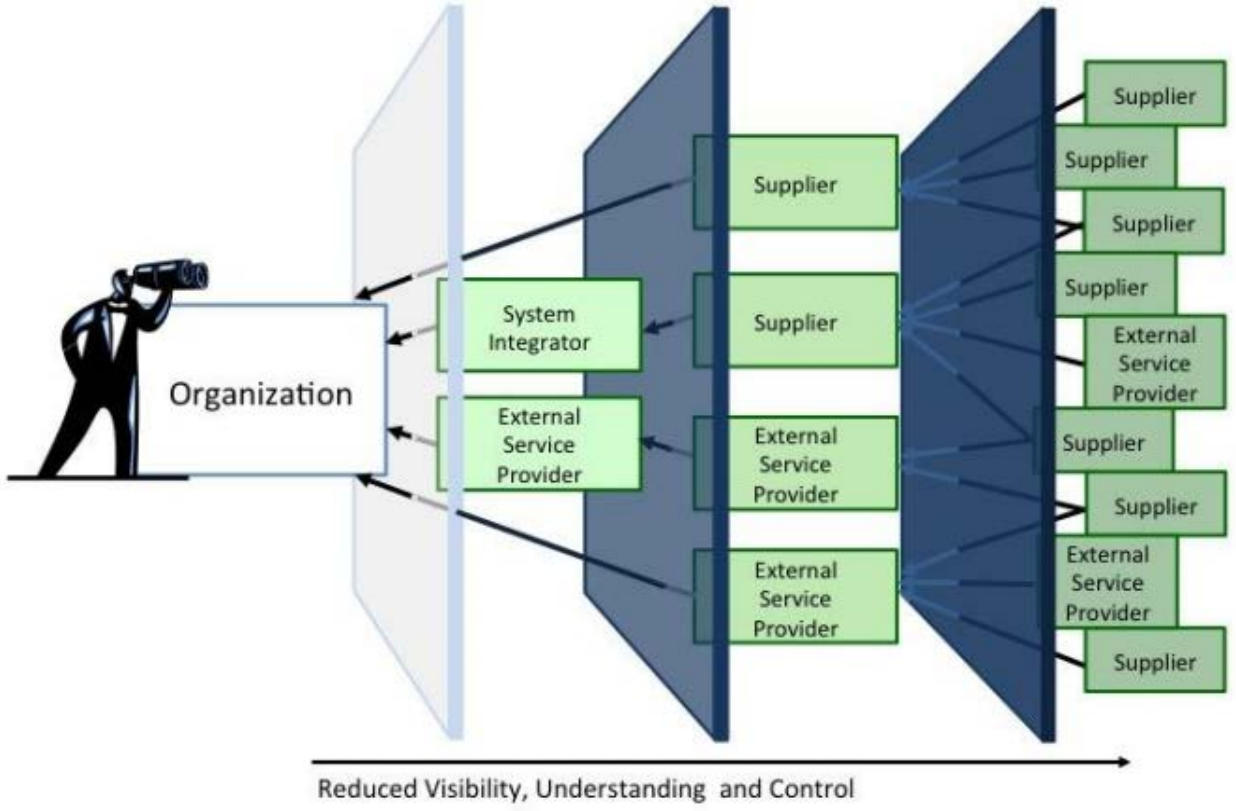
What makes The SolarWinds Breach Different?

Occurred during the application development phase

- One of the a growing number of compromises that occurred during the development lifecycle
  - The affected code was part of a trusted, digitally signed piece of commercial software
- SolarWinds software is an industry-leading suite of network management applications
  - Operates at an elevated privilege level
  - Estimated to have been deployed to over 18,000 businesses and federal agencies
- The SUNBURST “Trojan” did not interfere with normal application functionality
  - It tested its environment first, to make sure the application was actually deployed on an enterprise network
  - Code strings were purposely obfuscated & communications traffic was designed to mimic expected traffic patterns
  - Backdoor connectivity provided attackers with “hands-on-keyboard” remote access
- SUNBURST likely has been in production since March 2020
  - Consider the impact of, and recovery process for, a system compromise that’s was ongoing for 9 months!
- There is significant risk that other industry-leading software development firms have suffered similar development cycle compromises
  - We probably know this Trojan exists today, and many details of how it operates, only because the attackers targeted a security research firm
  - There is some evidence suggesting SolarWinds used popular software development tools that may have played a role in the breach

Securing the Unknown

We face an ever-increasing reliance on complex pieces of software that cannot be fully validated



BPM

Source: **Supply Chain Risk Management Practices for Federal Information Systems and Organizations**
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

Supply Chain/Vendor Risk Management

- Assume Confidentiality, Integrity, and Availability (CIA) are your problem
  - It’s your organization, but you’re just one more client to the vendor
- Periodically demand evidence of due care and due diligence
  - Hosting/Cloud Provider Certifications
    - Current SOC II/Type II for hosting, application, & cloud vendors
  - Evidence of Insurance
  - Evidence of Testing

Does the vendor exhibit a culture of cybersecurity?

BPM

Pre-Purchase Vendor Due Diligence

- Disclosure of ***All*** Development Supply Chain Risks
  - What portions, if any, of the design and development process was/is outsourced?
    - What controls does the vendor have in place to manage their 3rd-party outsourcing risk?
    - What controls are in place to secure access to source code repositories?
    - Have any elements of the code base been re-used from code-sharing resources?
- Disclosure of ***All*** Support and Patch/Update Requirements
  - How is remote access for support handled?
  - How is patching/updating/change management handled?
  - What ports are listening for remote support & patching?
    - Can handshake attempts be restricted?
      - By source IP address, certificate, MAC address, etc.
- Disclosure of ***All*** Communications Protocols
  - What type (by protocol) and volume of internal traffic is expected?
  - What inbound/outbound ports will be used?
    - Can communications be restricted by source address, certificate, MAC address, etc.?
    - How much traffic is expected over these ports?
- Disclosure of ***All*** Required Accounts
  - What are all the accounts, e.g. user, admin, supervisor, etc.?
  - Are there any undocumented accounts?
  - What are the privilege levels for all the different accounts?

BPM

Pre-Purchase Vendor Due Diligence, cont.

- Disclosure of ***All*** Encryption Controls
  - Are all data encrypted in transit?
    - Any unsigned or misconfigured certs?
    - Any weak ciphers or hashing algorithms?
  - Are all sensitive data encrypted at rest, considering Hypervisor, Container, OS, DB, & File levels?
    - Database data?
    - Backup files?
    - Credentials in process memory, e.g. RAM?
    - Windows registry, e.g LSA Secrets?
    - Session keys?
    - Are passwords hard-coded into the application?
    - Configuration files, e.g. .config, .ini, etc.?
    - Log files?
- Disclosure of ***All*** Access Controls
  - What are minimum password requirements and are they configurable?
  - Is Multi-factor Authentication supported?
  - Is Single Sign-On supported?
- Disclosure of ***All*** Integrity Controls
  - Is SMB signing supported?
  - Is LDAP signing supported?
  - Does the development process implement code signing?
- Permission to Include the Vendor's System in the Organization's Testing Regimen?
  - Or demand evidence of the vendor's ongoing test regimen

BPM

Additional Risk Management Guidance

Transferring Risk & Cyber Liability Insurance

- What Systems Are Covered?
  - Mobile devices?
  - Vendor owned/managed systems?
  - Contractor hosts?
  - Cloud systems and applications?
  - Biomedical & Industrial Control systems?
- Are There Exceptions to Coverage Related to Inadequate Due Diligence/Due Care?
  - Inadequate vendor management?
  - Inadequate patch & configuration management?
  - Inadequate risk assessment/penetration test program?
  - Inadequate program documentation?
  - Inadequate employee awareness & board/executive governance training?
- What Constitutes a Covered Data Security Breach?
  - Is a social engineering attack covered?
  - Is a ransomware attack covered?
  - Is a physical attack covered?
  - Is an inadvertent PII disclosure covered?
  - Is a state-sponsored act covered?
  - Is a prior act covered?
  - Are losses outside the breach event covered, e.g. client-led class-action suit?
- What Will the Policy Pay For?
  - Business interruption costs?
  - Reputation loss costs?
  - Legal fees?
  - Regulatory claims & fines?
  - Forensics & recovery costs?
- Are There Any Overlapping Provisions, *e.g.* business interruption also covered by property policy?
- Be Brutally Honest Filling Out the Application/Questionnaire
  - Your claim may be denied for a fraudulent application

BPM

Safe Computing Tools & Techniques

Password Management

- Use strong passwords
  - Length is the most important criterion for a strong password
  - It must also be difficult to guess
- Store them in password vault applications
  - KeePass, RoboForm, etc.
  - Or at least password protect that Excel file you're using…☺
- Put up with the hassle of multi-factor authentication
  - Google Authenticator, Duo, RSA, etc.

Email

- Don't use email for sensitive information!
  - Many message/chat platforms use end-to-end encryption
  - Password protect attachments
  - Sanitize the contents of your inbox, sent, trash, etc.
  - Use inbound mail filter tools to pre-examine attachments and links
    - For personal email, see apps like Hushmail
- If you must use email for sensitive data, use encryption tools
  - GPG
  - Zixmail

BPM

Safe Computing Tools & Techniques

Browsing

- Before logging in, confirm the word immediately preceding the .com, .org, .net, etc. and the .com itself

  https://www.**chase**.com vs. https://www.**chase.bank**.com

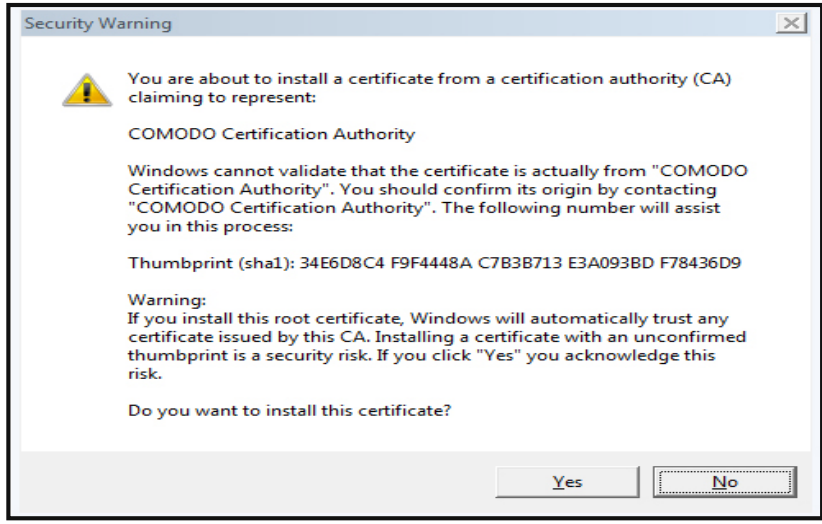
  https://www.chase.**com** vs. https://www.chase.**net**

- Logout when you're done

- Secure your browser settings, *e.g.*
  - Firefox with
    - No-Script (prohibits a startling number of scripts running in the background)
    - Privacy Badger (restricts ads, cookies, tracking)
    - Foxy Proxy (hides your point of origin)

- Limit sharing & post anonymously, whenever possible
  - Yelp & Google Review Scams

- Be suspicious of all popups & dialog boxes



A common online banking attack toolkit asks the user to install a malicious root certificate

Social Engineering Warning Signs

- Requests anything out-of-the-ordinary
  - Offer to help with problem you didn't know you had
  - Offer that sounds too good to be true
- Name-drops, claims of authority, or urgency
  - Cavalier or superior attitude
- Compliments, flatters, or flirts
- Promises reward or threats for non-compliance
- Refuses, or gets uncomfortable, when asked to provide supporting information
  - Government-issued ID (never trust a business card)
  - Callback # (never trust CallerID)

Review of Social Engineering Defenses

- Establish a Culture of Cybersecurity
  - Security starts at the top, but it is everyone's job
  - Test, train, repeat
- Telephone Attacks
  - Train live receptionists to recognize suspicious and repeat calls
  - Verify purpose of the call and permission to disclose
    - Have a prepared response
  - Verify the phone number
    - Caller ID check via dial-back
  - No sensitive information should be disclosed
    - Learn what is sensitive information and where it resides
- Email Attacks
  - Always confirm sender - hit "reply" to see if return address matches (alleged) sender
  - Never enter credentials on an unrecognized URL - without an explicit IT directive
  - Do not open suspicious attachments – have IT examine them first
  - Hover over links, and verify destination URL, before clicking – do not click on unrecognized URLs
- Onsite Attacks
  - Challenge unknown persons politely, or report them!
    - Collect business card - inquire purpose of visit
    - Check driver's license as positive photo ID
    - Verify purpose and scope of visit with appropriate managers
    - Log visit
    - Escort visitors at all times

Parting Shot:
Everyone Is the Security Officer

- Follow secure practices
  - Passwords
  - Email
  - Browser
  - Remote Access
  - etc.
- Make Cybersecurity part of the conversation
- Thank employees, customers, and business associates for putting up the inconvenience of Infosec safeguards and remind them we're all in this together

BPM

Conclusions

- The cybersecurity threat landscape is worsening
  - Threat sources include hacktivists, cyber criminals, nation-state sponsored entities, and insiders
  - Hackers employ a combination of human, physical, and technological attacks
    - Many current and evolving threat scenarios involve social engineering and/or sophisticated technical supply chain attacks
  - Effective Risk Management requires awareness and strong controls – balanced against convenience and user satisfaction

BPM

BPM

Thank You!