TOUCHSTONE SECURITY

Hybrid Work and Cyber Security for Small and Medium-sized Business

Rich Shinnick

Richard Shinnick, former **NSA advisor** and **Air Force veteran**, is the Founder of Touchstone Security. Mr. Shinnick has **35+ years of experience** in the computer security industry providing advice on the risks associated with information technology with a specialty focus on cloud technology. For a decade Mr. Shinnick developed and taught Cyber Security courses at **Columbia University**, **New York University**, the University of Barcelona, and Borough of Manhattan Community College. Clients include **Goldman Sachs, Bank of New York, and LBBW**. Mr. Shinnick served in the United States Air Force Electronic Security Command as an Airborne Cryptologic Linguist in the Rivet Joint Program during the Cold War. He holds a B.S. degree in Professional Aeronautics from Embry-Riddle Aeronautical University.

Deep Experience

- Military Trained Team
- Best in Breed Solutions
- Relationship Centric Approach
- Decades of Experience

We are proud to serve:

Goldman Sachs

Columbia University

NJ TRANSIT The Way To Go.

IBM

Disney

Raytheon

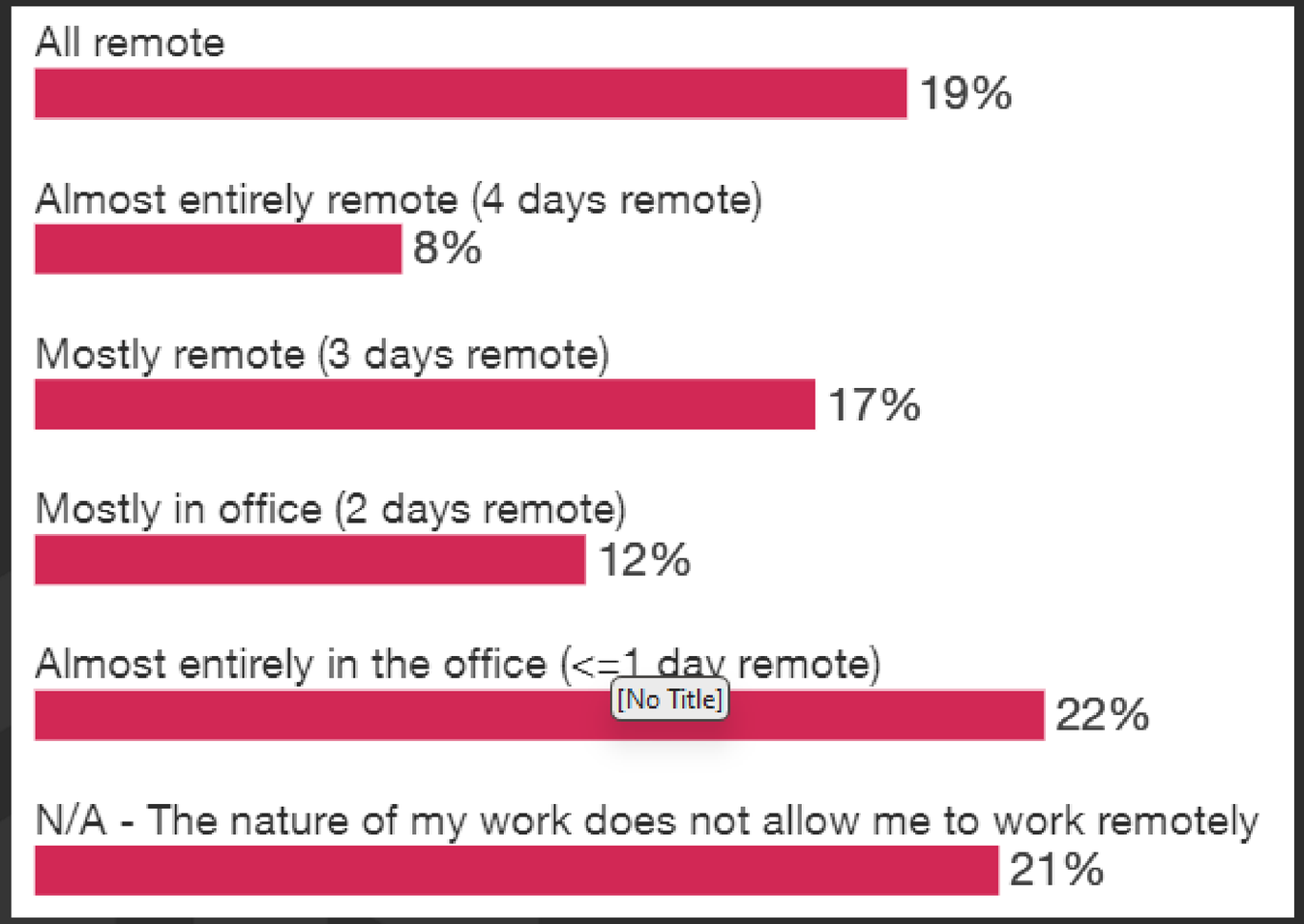
TOUCHSTONE SECURITY

Agenda

- Employee Preferences for Hybrid Work
- The Hybrid Workplace
- Staggering Statistics
- Verizon Data Breach Investigations Report (2022 DBIR)
- CIA
- Cybersecurity Recommendations for SMBs
- Multi Factor Authentication
- Awareness Training
- Avoiding High Risk
- CISO Recommendations
- Zero Trust
- Tips and Tricks
- Ransomware Attacks
- Tech Support and Phone Scammers

Employee Preferences for Hybrid Work

Source: PwC US Pulse Survey, August 19, 2021: base of 1,007 full-time and part-time employees



TOUCHSTONE SECURITY

The Hybrid Workplace

- **81% of enterprise organizations** have begun the move to a hybrid workplace with **31% already fully adopted** (Microsoft).

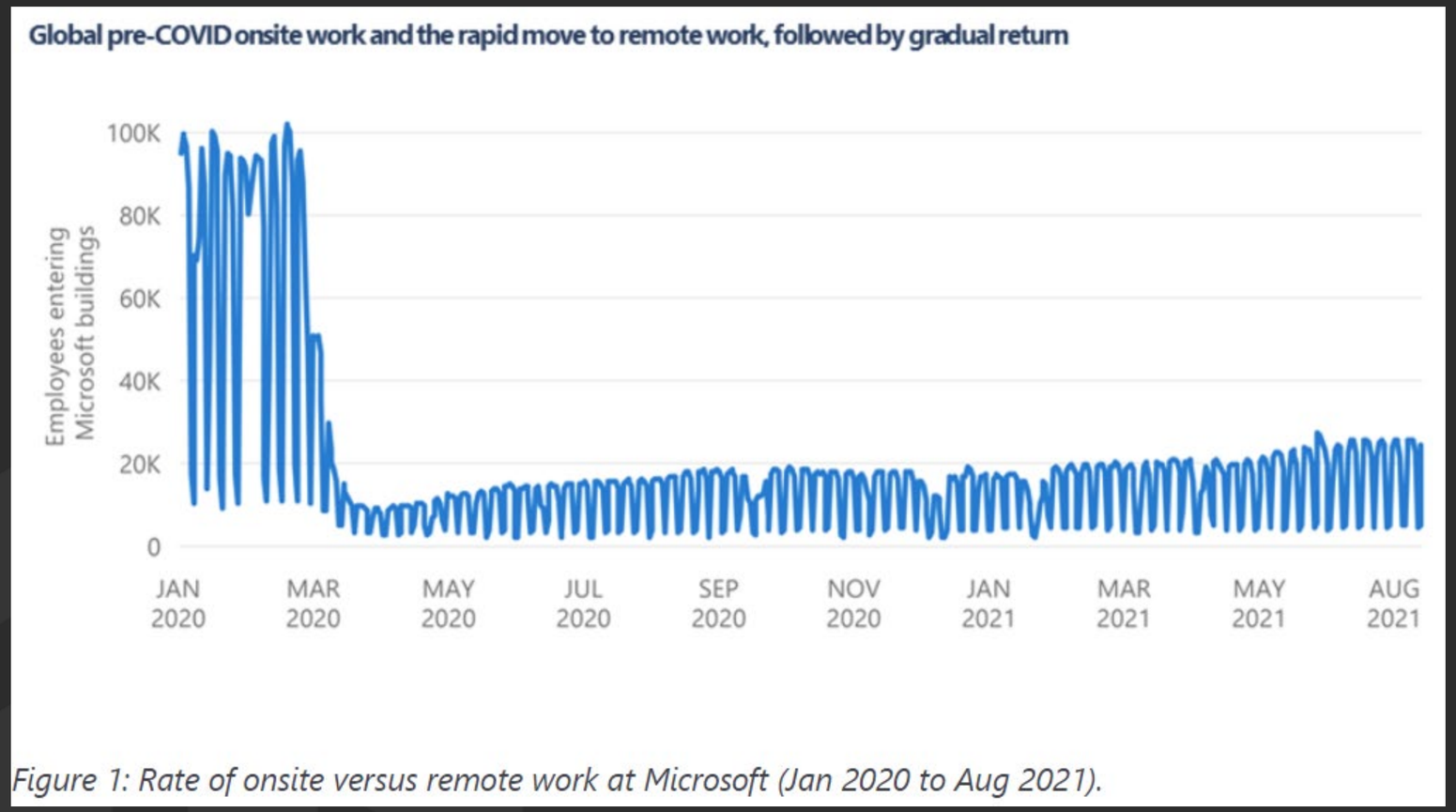


Figure 1: Rate of onsite versus remote work at Microsoft (Jan 2020 to Aug 2021).

TOUCHSTONE SECURITY

The Statistics are Staggering

- Most CISOs reported a **significant increase** in cyberattacks (higher than 70%) (E&Y)
- **86%** of CISOs reported a successful cyberattack in 2021 (E&Y)
- **>70%** of data breaches were **financially motivated** with more than 25% involving insiders (E&Y)
- Each year brings record breaking numbers of attacks and damage
  - LinkedIn, Facebook, Microsoft, Solarwinds, Capital One, etc.
- 13% year/y increase in **ransomware** attacks, a jump greater than the past 5 years combined (DBIR)
- Roughly **4 in 5** breaches can be attributed to **organized crime**, with external actors approximately 4x more likely to cause breaches in an organization than internal actors (DBIR)
- **82%** of all breaches analyzed over the past year involve **the human element** (DBIR)
- 43% of **people have made mistakes** at work that compromised cybersecurity (Tessian)
- 25% of employees said they have clicked on a **phishing email** at work. Men were twice as likely as women to fall for phishing scams, with 34% of male respondents saying they have clicked on a link in a phishing email versus just 17% of women.

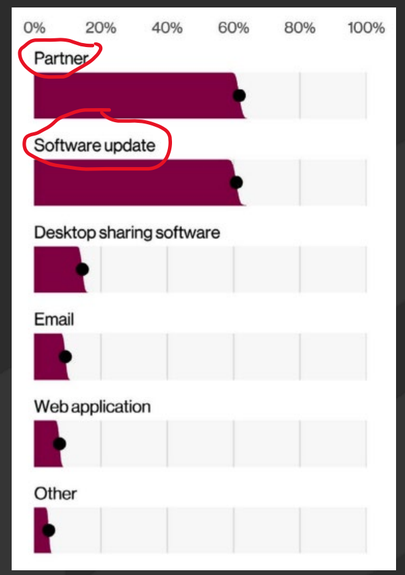
The Statistics are Staggering

- **93%** of company networks **can be penetrated** by Cybercriminals (Pentester Positive Technologies)
- **71% of companies hacked via CREDENTIAL COMPROMISE**
- The most common causes of cyber-attacks are malware (22%) and phishing (20%)
- Cybercrime cost U.S. businesses more than $6.9 billion in 2021
- **89%** of organizations are being targeted by email and phone fraud scams (Abnormal)
- **84%** increase in # of Business Email Compromise (BEC) attacks in second half 2021 (Abnormal)
- 72% chance of *receiving a phone fraud attack* **each week** for large enterprises (Abnormal)
- 66% of organizations surveyed were hit with **ransomware** in 2021, up from 37% in 2020 (Sophos)
- $812,360 - the average ransom paid by organizations that had data encrypted in their most significant ransomware attack, increased nearly fivefold

DBIR - Breach Patterns over time

2022-data-breach-investigations-report-dbir.pdf (verizon.com)

Frequency	7,013 incidents, 1,999 with confirmed data disclosure
Threat Actors	External (98%), Internal (2%) (breaches)
Actor Motives	Financial (93%), Espionage (6%) (breaches)
Data Compromised	Credentials (42%), Personal (37%), Other (35%), Internal (16%) (breaches)



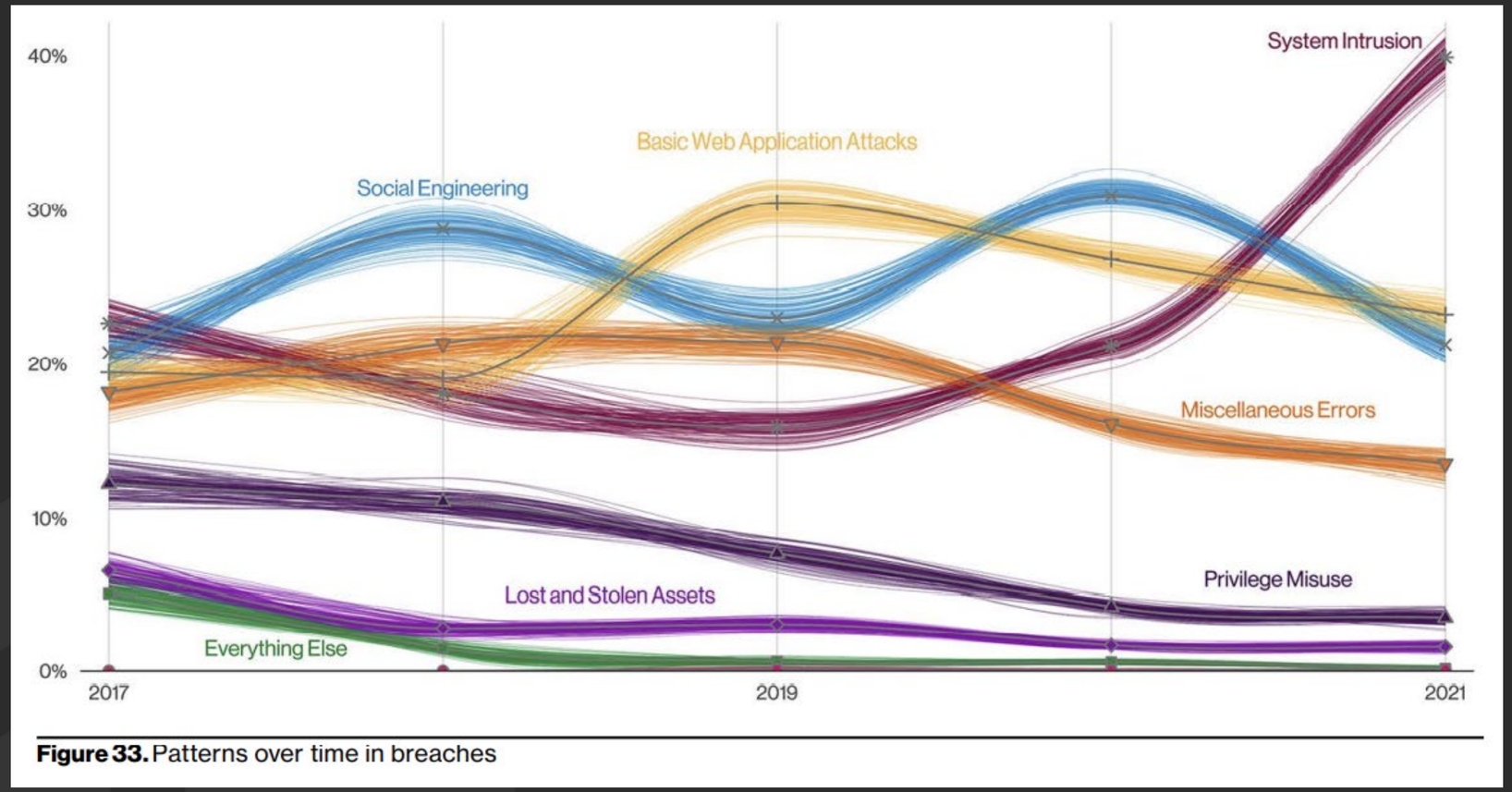


Figure 33. Patterns over time in breaches

TOUCHSTONE SECURITY

DBIR – Ransomware Breaches over time

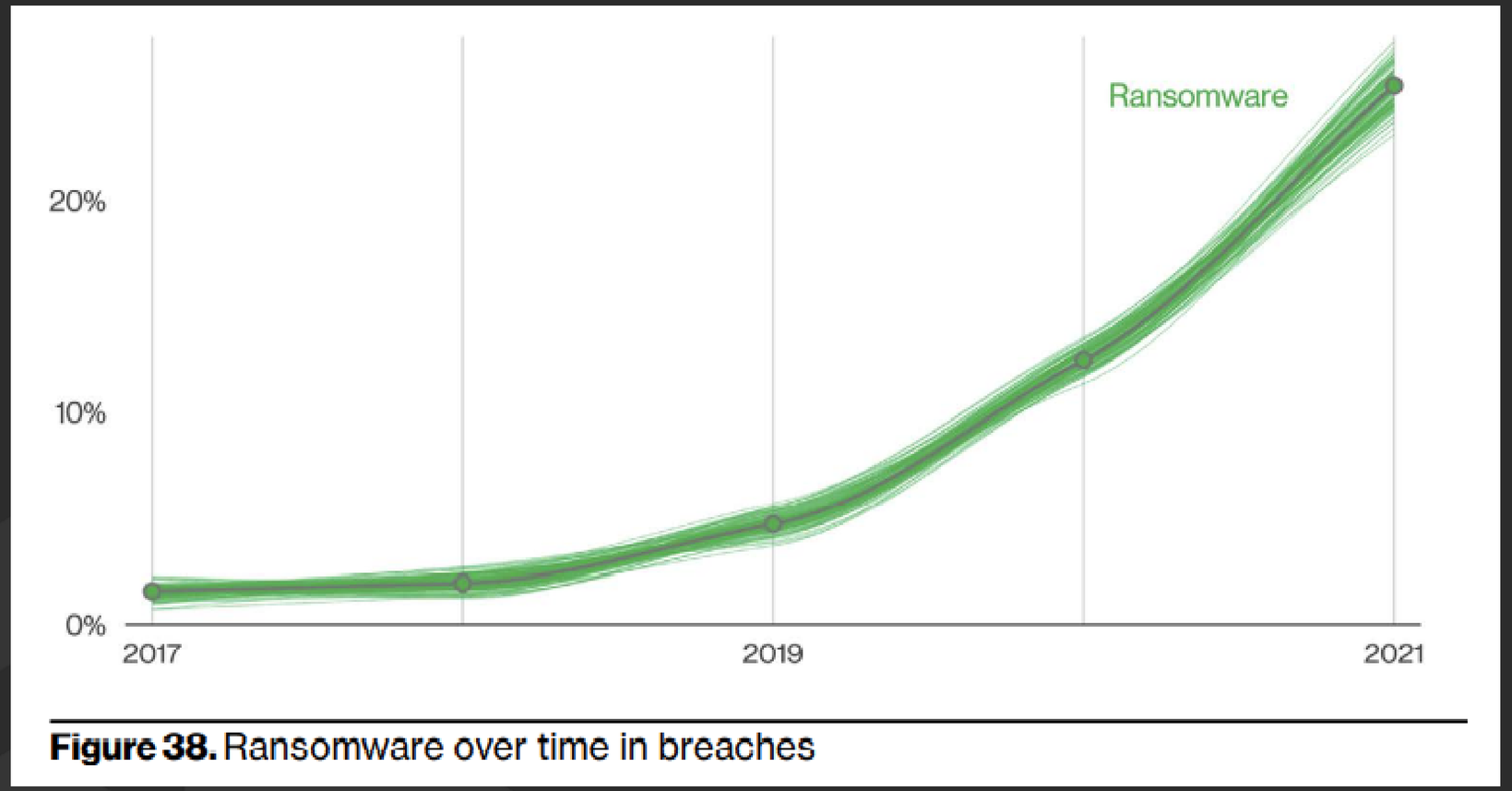


Figure 38. Ransomware over time in breaches

TOUCHSTONE SECURITY

DBIR - Ransomware Incident Varieties

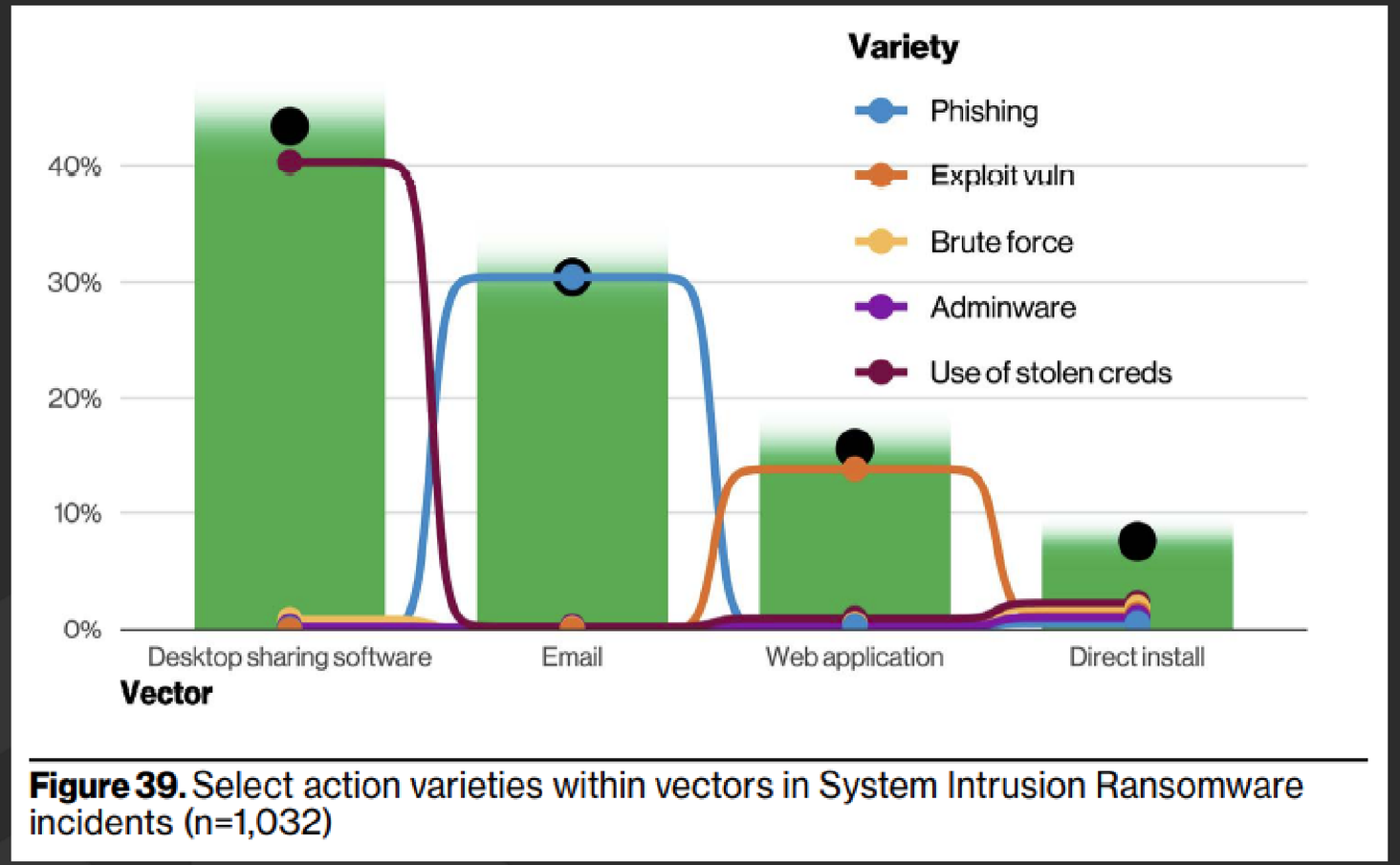
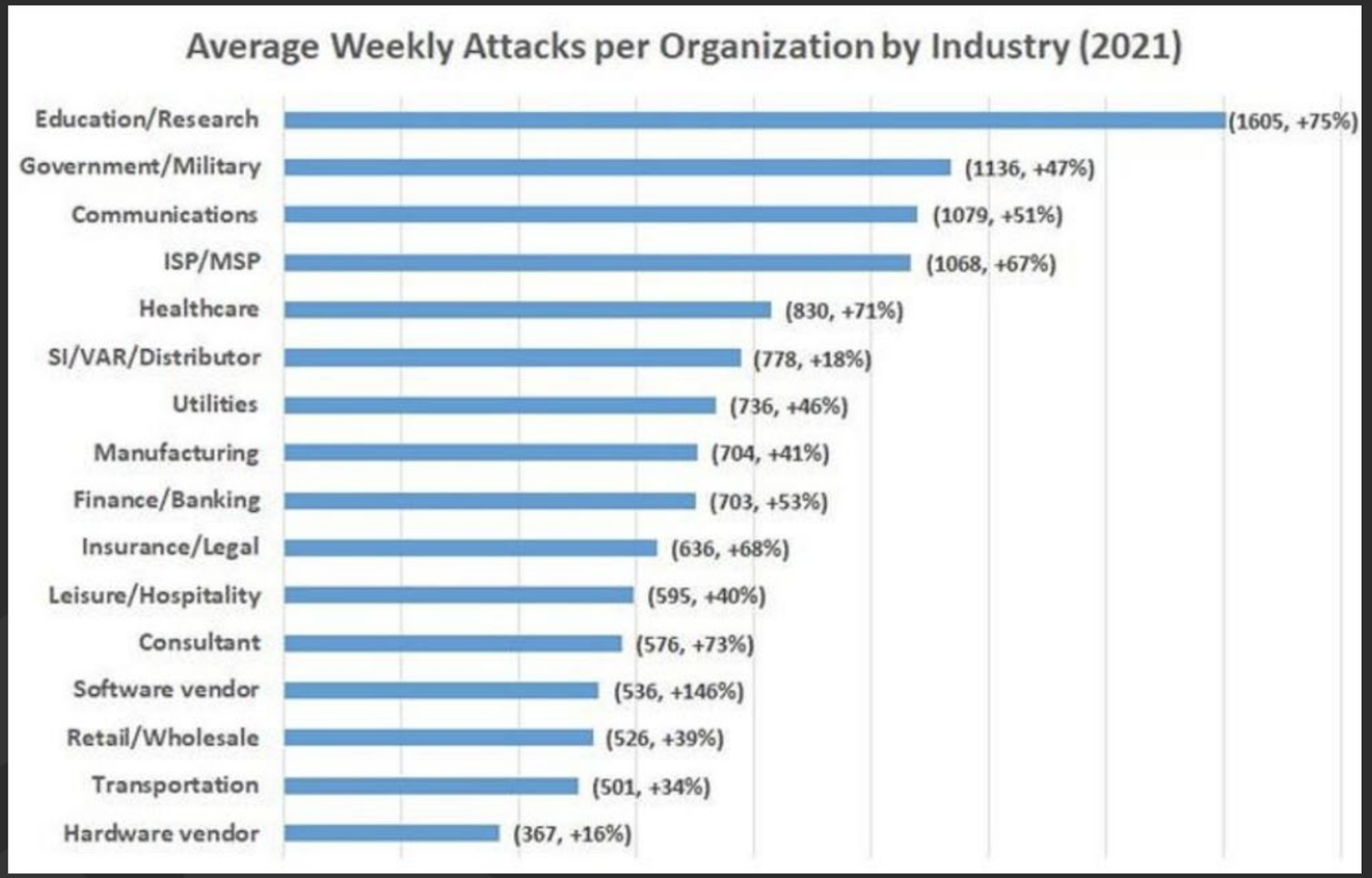


Figure 39. Select action varieties within vectors in System Intrusion Ransomware incidents (n=1,032)

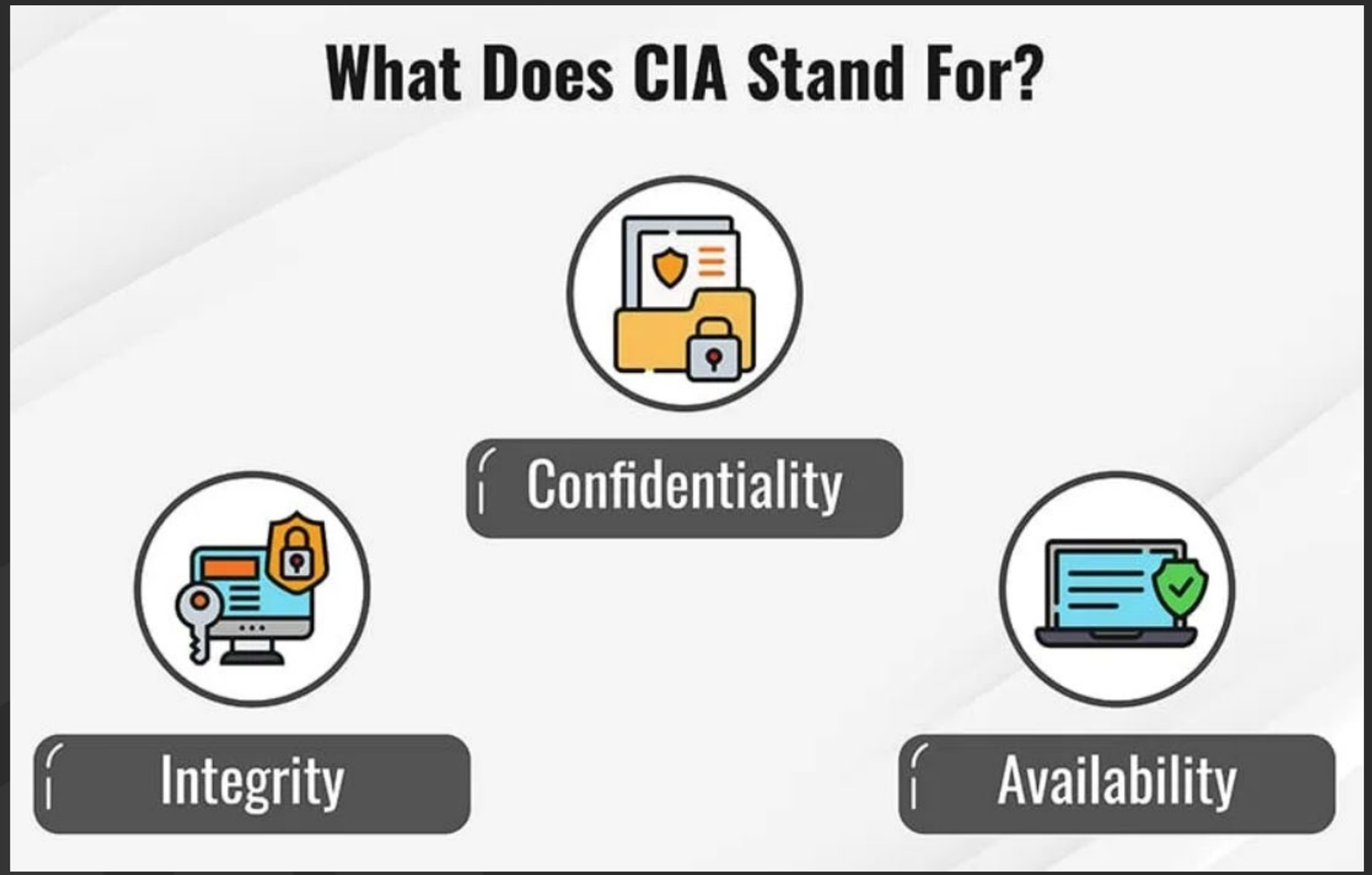
TOUCHSTONE SECURITY

Attacks per Organization



TOUCHSTONE SECURITY

What do we protect?
CIA Triad



TOUCHSTONE SECURITY

Small SMB Recommendations

- **Raise Awareness** amongst all employees (make it part of your culture)
- Implement MFA (Multi Factor Authentication) everywhere
- Use a password manager (1Password, Dashlane, Lastpass)
- Do not reuse or share passwords
- Change default credentials on all equipment & follow vendor security guidance
- Back up all data offline regularly (not USB connected) (Can be cloud, but must include WORM)
- Ensure continuous software patch installations
- Implement Anti-phishing controls such as Barracuda Sentinel, Proofpoint, Microsoft Defender, others.
- Replace antivirus software with outsourced Endpoint Detection and Response (EDR)
- Stop allowing personal computers for employees (issue company managed systems)
- Implement a risk assessment process.

Small SMB Recommendations (cont.)

- Audit your environment and assess risk (use 3rd Party)
- Conduct Periodic Vulnerability Scans (consider 3rd Party)
- Consider a Yearly Penetration Test (see http://www.pentest-standard.org/index.php/Main_Page)
- Consider a Remote Monitoring & Management (RMM) (or outsource to an MSP/MSSP)
- Implement and maintain an Information Security Program (ISP)
- Start implementing Zero Trust, do not wait
- Implement Web Filtering
  - Malwarebytes offers a free filtering tool
  - Most firewalls have this feature
- Subscribe to Intelligence Threat Feeds
  - FBI InfraGard Home (infragard.org)
  - Open source threat feeds / block lists for firewall rules
    - https://rules.emergingthreats.net/blockrules/compromised-ips.txt
    - http://cinsscore.com/list/ci-badguys.txt
    - https://www.blocklist.de/en/index.html
    - URLhaus | API (abuse.ch)

Small SMB Recommendations (cont.)

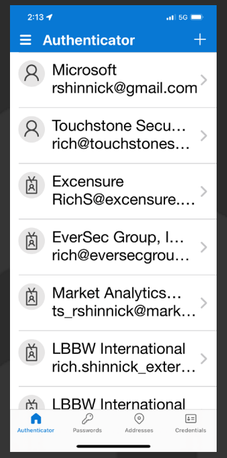
- Implement **segmentation** (e.g. Development environment completely isolated from production; Sensitive systems isolated; DMZ)
- Check your website's SSL at SSL Server Test (Powered by Qualys SSL Labs)
- Implement proper email DNS entries (DKIM, DMARC, SPF, https://mxtoolbox.com/
- Separate sensitive "in scope" systems from non-essential systems
- In scope systems are systems that must be complaint to relevant standards/regulations
- In scope includes systems that have access to sensitive/classified data

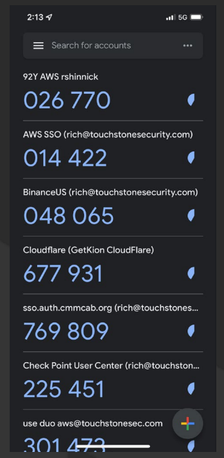
Multi Factor Authentication

1. Something you know
2. Something you have
3. Something you are

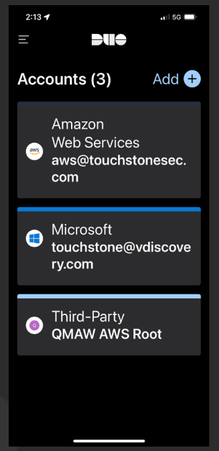
Many of these MFA solutions integrate with Facial Recognition and leverage the TPM 2.0 standard.

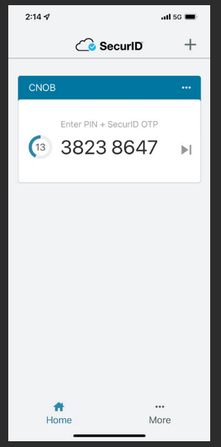
Microsoft Authenticator
Google Authenticator



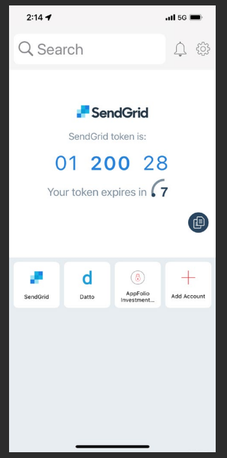


DUO
SecurID





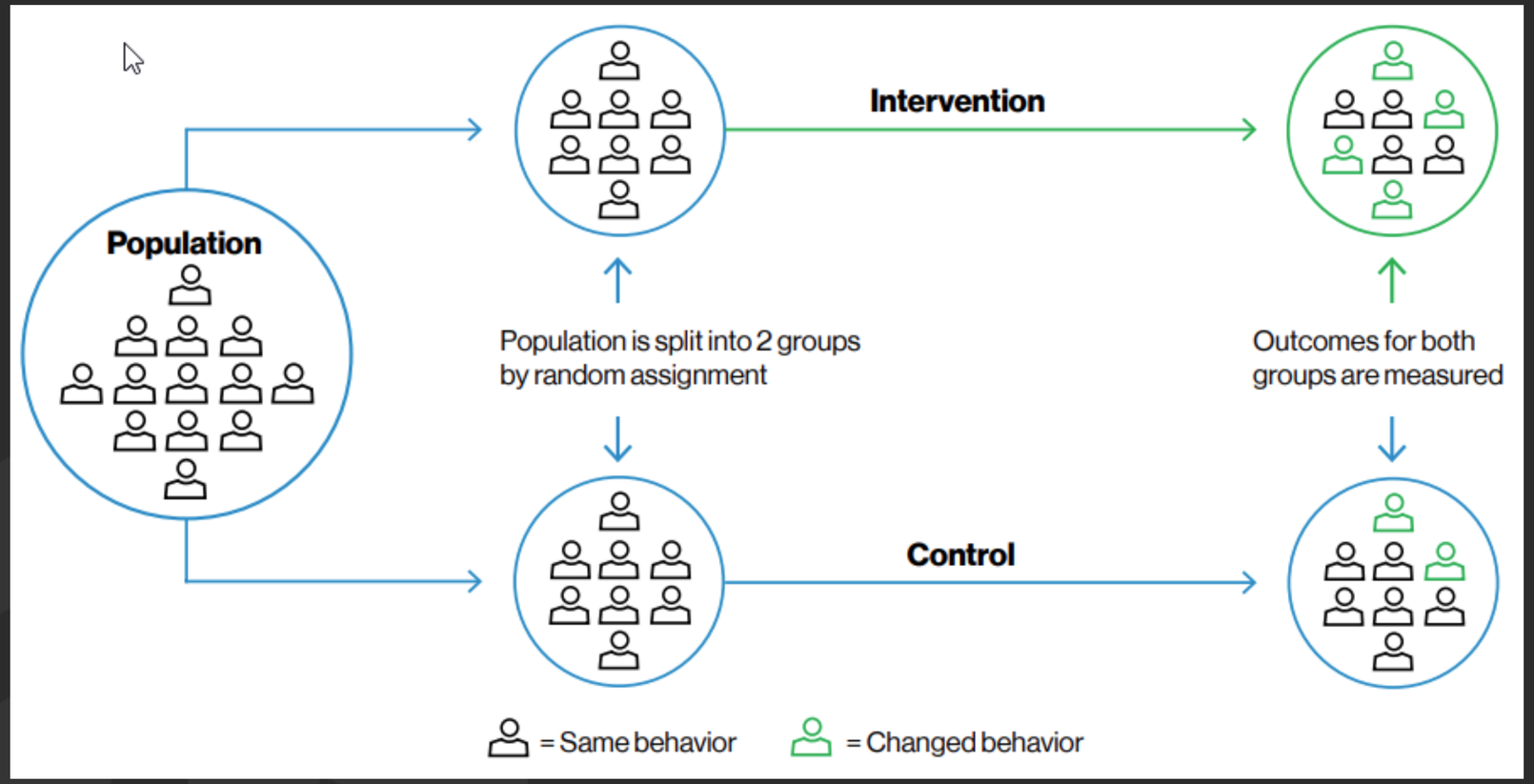
Adobe
Authy



TOUCHSTONE SECURITY

Changing Behavior – Awareness Training

- Humans make mistakes! How do you affect change? Cybersecurity Awareness Training.
- DBIR reported that the **human element impacted 85% of breaches** in 2021, and 82% this year.



TOUCHSTONE SECURITY

Avoid High Risk

- Avoid Non-company owned and controlled computers (NO PERSONAL COMPUTERS ALLOWED)
- Implement a central, automated software patching system
- Implement a centrally managed EDR (Endpoint Detection & Response) system
- Practice Least Privilege (No admin access - use separate “admin” accounts & change control)
- Don’t allow SSLVPN Split Tunnel; Implement endpoint checks, Web Filtering, and threat feeds
- Ensure mobile devices are encrypted with at least 256-bit.
- Train Employees (especially those who have poor cyber hygiene)

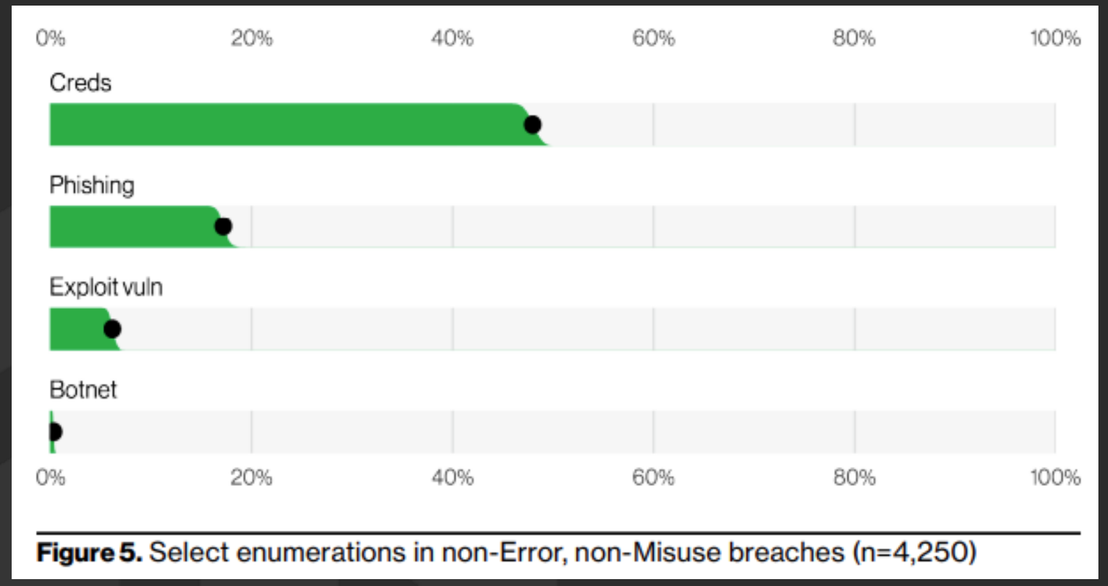


Figure 5. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

TOUCHSTONE SECURITY

Chief Information Security Officers (CISO's) what to do?

- Get buy-in from the top – then communicate it (incorporate into culture)
- Implement and maintain an Information Security Program (ISP)
  - Implement Change Control for all technology changes
- Change employee mindset (Awareness Training – find the weakest link)
- Audit your environment and assess risk (use 3rd Party)
  - Conduct Periodic Vulnerability Scans
  - Consider Yearly Pentests (see http://www.pentest-standard.org/index.php/Main_Page
- Maintain a Remote Monitoring & Management (RMM) system
- Migrate to the cloud.
- Adapt Cloud-based IAM systems integrated with MFA.
  - Azure Active Directory and Google Cloud Identity are cloud-based identity and access management services used in the hybrid workplace.
  - Google and Microsoft's Cloud-based IAM systems are used by thousands of other SaaS applications.
  - SaaS systems (such as Salesforce, Hubspot, Slack, etc.) can integrate with IAM.
- Start implementing Zero Trust

Get Buy In from the Top

- Almost **90%** of senior managers regularly uploaded work files to a personal email or cloud account (Stroz Friedberg)
  - More than half had accidentally sent the wrong person sensitive information and had taken files with them after leaving a job.

WHY?

- No patience for security measures (e.g. MFA, VPN);
- Travel a lot to places with poor Internet connectivity;
- Refuse to change passwords;

Cyber Insurance Harder to get

- Prices have soared amid increased ransomware hacks and others
- Insurance companies are asking for policies and procedures, etc.
- **79% increase in prices** from a year earlier (Marsh & McLennan Global Insurance Market Index)
- **92% increase in price** of Direct-written premiums from 2020 (National Association of Insurance Commissioners)

Prioritize Initiatives

- Address the weakest link – the human element
  - Implementing Multi Factor Authentication
  - Training employees with Awareness Training
- Replace legacy system(s), keep them patched until then
- Make sure your IT Support (ISP/MSP) is cybersecurity fluent.
- Seriously consider a 3rd party MSSP for xDR and 24x7 SOC
- Execute on Zero Trust

Zero Trust

- Zero Trust is: “Never trust, always verify”.
- Bring Your Own Device (BYOD), firewalls and Virtual Private Networks (VPN) do not support Zero Trust natively. Conditional Access is required.
- Conditional Access – requires certain “conditions” to grant “access”.
- Conditions include MFA, user identity in a group (“finance group”,) IP Location (“geo fencing” – only in US), Device (only company issued machine), Real-time and calculated risk detection (user was signed in at noon in NY, then tried to login from CA), endpoint compliance (encryption, patch state, OS version, EDR).

Deployed across 6 areas

1. Identities
2. Endpoints
3. Applications
4. Network
5. Infrastructure
6. Data

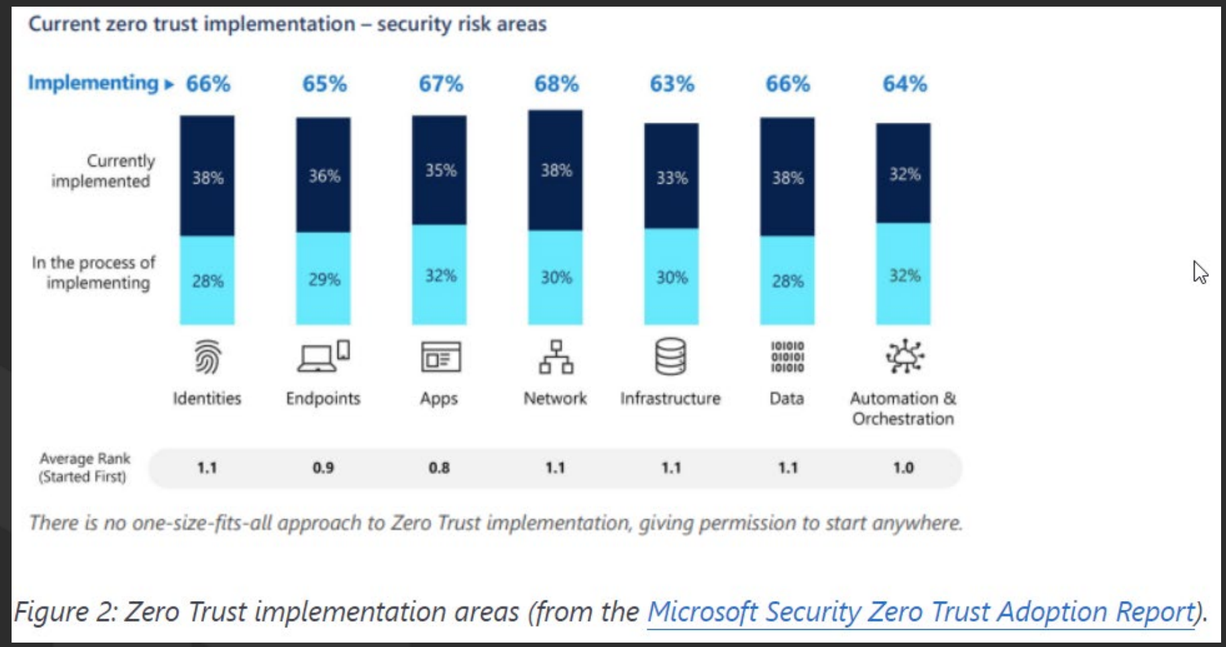


Figure 2: Zero Trust implementation areas (from the Microsoft Security Zero Trust Adoption Report).

TOUCHSTONE SECURITY

1. Identity – 61 million password attacks daily Azure AD

- Identity includes people, services, and Internet of Things (IoT)
- Multi Factor Authentication (MFA) can protect against 99.9% of identity attacks
- Passwordless authentication is the best
- Legacy authentication (used with legacy protocols such as IMAP, SMTP, POP, and MAPI) do not support MFA)

2. Endpoints

- Only allow access from company managed devices
- Grant access to sensitive applications from a subset of company managed devices
- Validate device is running the latest operating system and software patches
- Validate device is running latest security software with no risks found
- Implementing a Mobile Device Management solution such as Microsoft InTune or Google Endpoint Management
- Consider implementing a Network Access Control (NAC) system

3. Applications

- If modern, should support and use MFA
- If not capable of MFA, you should (1) upgrade, (2) migrate to SaaS, (3) utilize application tiers (Webserver, App, DB on separate segments)
- If legacy, implement “compensating controls”, such as a reverse proxy, Secure Access Service Edge system (SASE), micro-segmentation

4. Network

- Avoid a “flat” network – implement segmentation (vLANs, DMZs, etc.)
- Have a plan to protect against a Distributed Denial of Service (DDoS) attack
- Leverage Unified Threat Management (UTM) features in your firewalls
- Consider Network Detection & Response solutions (IDS/IPS, NDR)

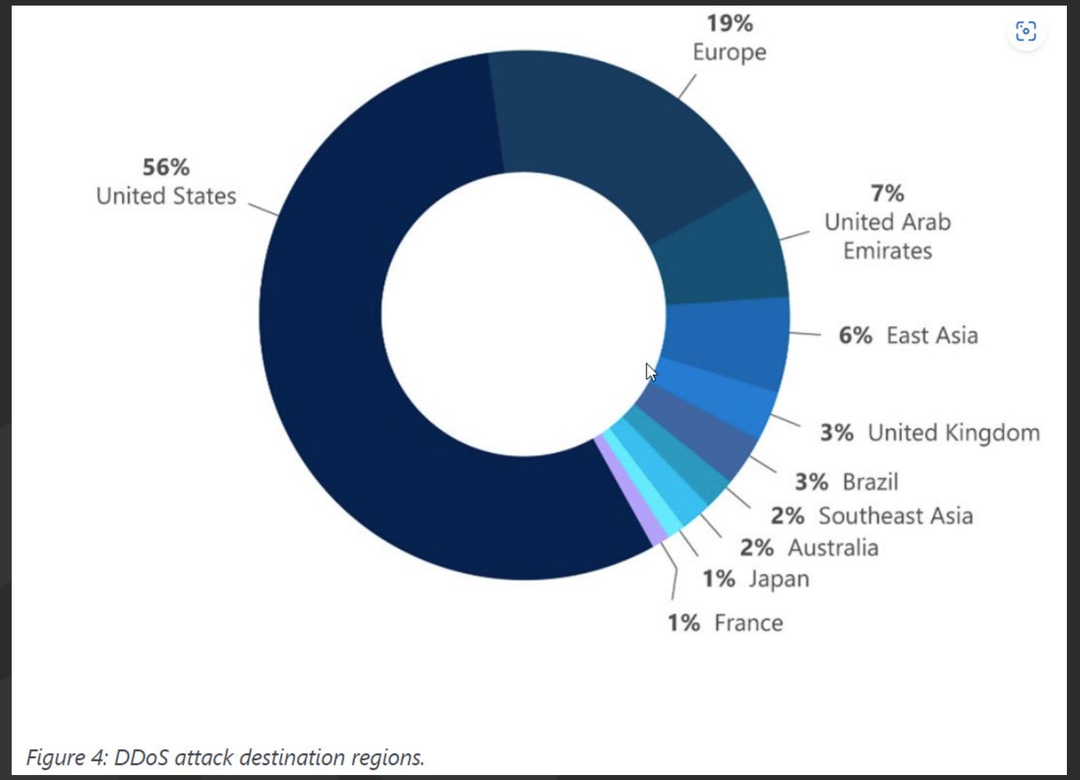


Figure 4: DDoS attack destination regions.

TOUCHSTONE SECURITY

5. Infrastructure

- Infrastructure includes network devices, cloud environments (AWS, Azure, GCP), storage, virtual machines, containers, micro-services, Internet of Things, and telephony systems.
- These unique devices represent a critical threat vector.
- Ransomware Threat Actors target these systems.
- Special skills required to protect infrastructure.
- “Shared Security” model

- According to Gartner, **SaaS** “remains the largest public cloud services market segment, forecasted to reach **$176.6 billion** in end-user spending in 2022.” – SaaS is another attack surface to be protected.

6. Data

- Important that **data remain protected** during the entire lifecycle, from “at rest”, “in use”, “in motion”, all the way to “archived” and/or “destroyed”.
- Requires classification, labeling, encryption, data loss prevention, data leak protection, and destruction policies and procedures.

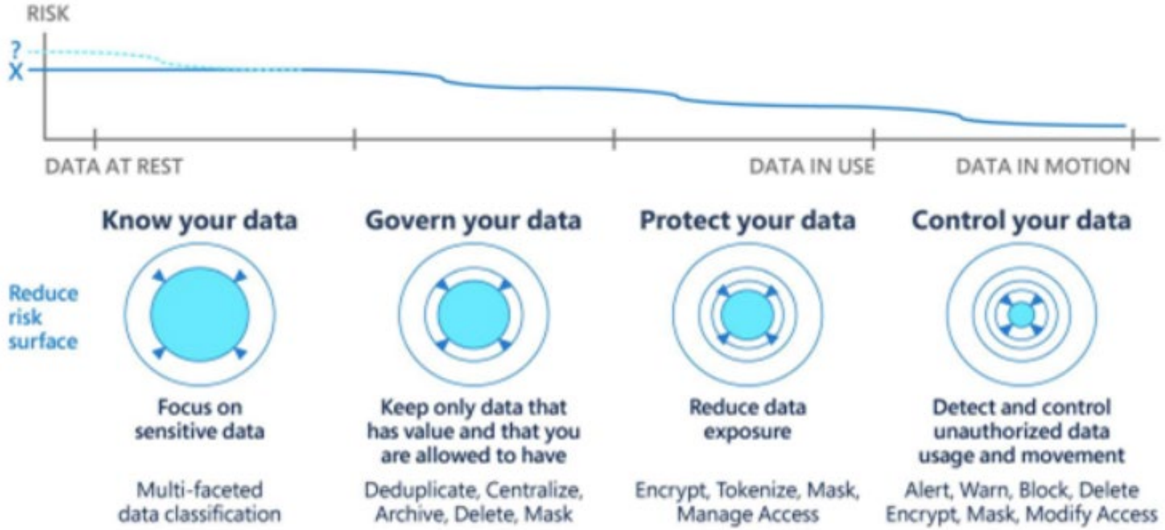


Figure 5. The cumulative impact of unified data governance and security on sensitive data risk.

TOUCHSTONE SECURITY

Tips and Tricks

- Use Windows built in Sandbox to safely run applications in isolation Windows Sandbox - Windows security | Microsoft Docs
- Read/review the Verizon 2022 Data Breach Investigations Report 2022 Data Breach Investigations Report | Verizon
- Install browser protection, such as Malwarebytes Browser Guard - Blocks ads, scams, and trackers
- Enable Hard Disk Encryption – Windows, LINUX, Chromebook, and Apple all include encryption, but you must enable this on Windows, LINUX, and Apple.

Ransomware Initial attack to full encryption < 4 hours

- Phone fraud on the rise – caller convinces user to download a file.
- A recent attack took all of 3 hours and 44 minutes to take control of all the servers (DFIR).
- Insurance companies are dropping Ransomware events.
- In a one-year research effort, researchers detected more than 1.2 million attacks per month.
- Increase in attacks across all of the most highly targeted industries, critical infrastructure 4x

Phishing, Brute Force and PowerShell Attacks Documented

Barracuda Networks detailed 3 “real-life” ransomware attacks in which the hackers used three different tactics to gain entry.

1. In one instance, the attackers used **a phishing email** sent in August 2021 to compromise one of the victim’s accounts.
2. In a second event, the attackers executed a **brute force attack on a VPN login page** and then used remote desktop protocol (RDP) to get into the compromised systems.
3. In a third case, the hackers got in with **stolen credentials** and then used malicious PowerShell scripts and installed system-level dynamic link libraries (DLLs) to steal more credentials and harvest passwords.

Scammers are getting better!

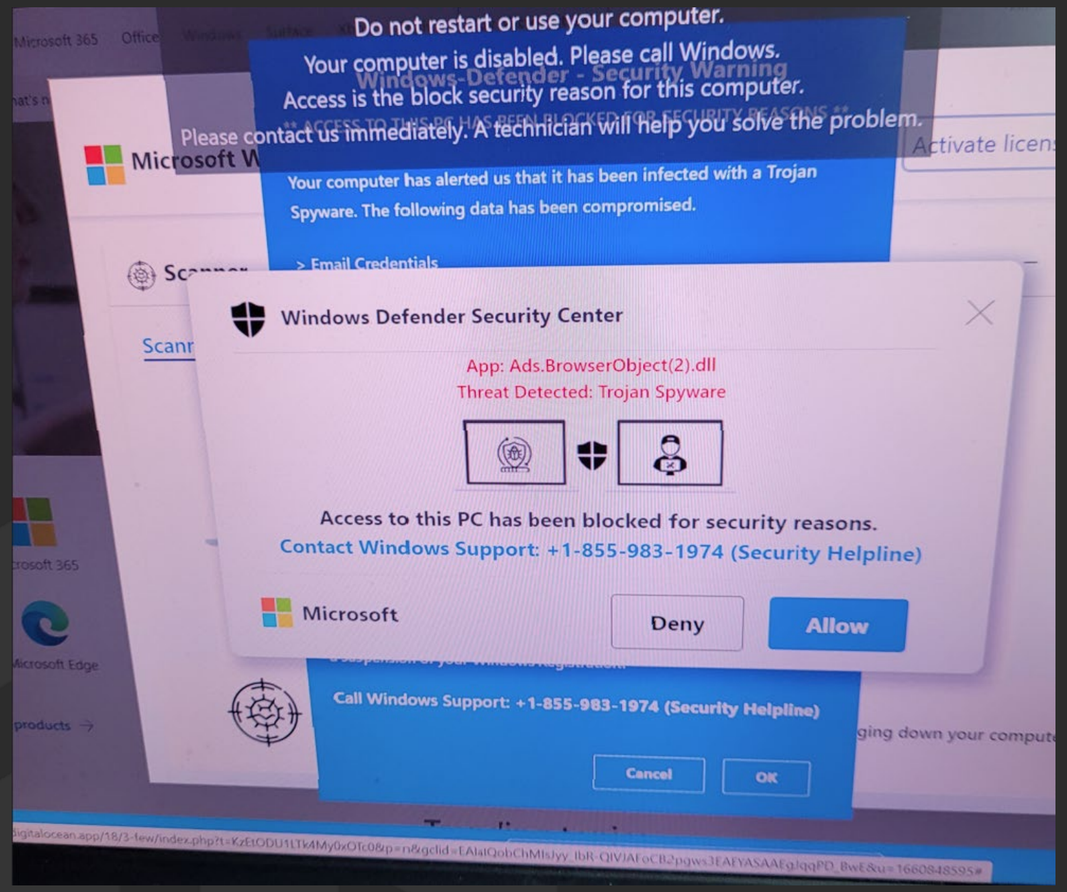
- Robocalls to your cellphone purporting to be from banks, Amazon, gift cards, stimulus check, IRS,
- There is a problem with your account!
- Nearly 1 in 3 Americans have fallen victim to phone scams (Truecaller)
- 19% fell victim more than once (Truecaller and The Harris Poll in March 2021)

What can you do?

- Never respond to a direct communication, always initiate communications via researched public contact information (be paranoid)
- Let the calls go to voicemail
- Block the number
- Use your home number when registering anything online (assuming you have a home landline), don’t use your cellphone

Tech Support Scamming

- Browser pop-up alerts with real looking screenshots
- Insisting you call a tech support line or click a link



TOUCHSTONE SECURITY

Conclusion

TOUCHSTONE
SECURITY

Why Touchstone?

- **Military Trained**
- **Deep Experience**
- **Responsive Team**
- **Touchstone has excellent references**
- **Touchstone is a certified Veteran Owned Business**