95% of cyber incidents are caused by human error.

Source: https://www.weforum.org/reports/global-risks-report-2022

Reducing the Human Error Rate

Jim Seaman, Director
IS Centurion Consulting Ltd

Agenda

- Leading An Effective PCI DSS Program
- Setting The Scene
- Understanding Human Failure
- Focus On The Human Factor
- Less Is More...
- A Time For Change
- Engage & Explain
- Turn Information Into Actionable Intelligence
- Think Beyond Compliance
- Cyber Security Statistics & Facts

PCI Security Standards Council®

Leading An Effective PCI DSS Program

Source: https://www.mindtools.com/pages/videos/leaderskillsquiz-transcript.htm

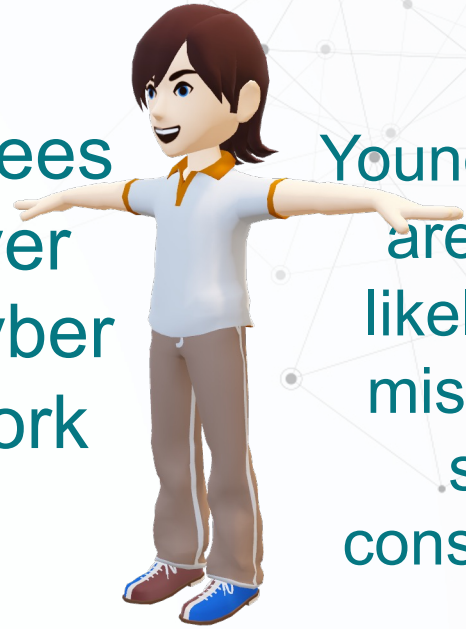
10 Common Leadership and Management Mistakes:
Avoiding Universal Pitfalls

1. Not Providing Feedback.
2. Not Making Time for Your Team.
3. Being Too "Hands-Off“.
4. Being Too Friendly.
5. Failing to Define Goals
6. Misunderstanding Motivation.
7. Hurrying Recruitment.
8. Not "Walking the Walk“.
9. Not Delegating.
10. Misunderstanding Your Role.

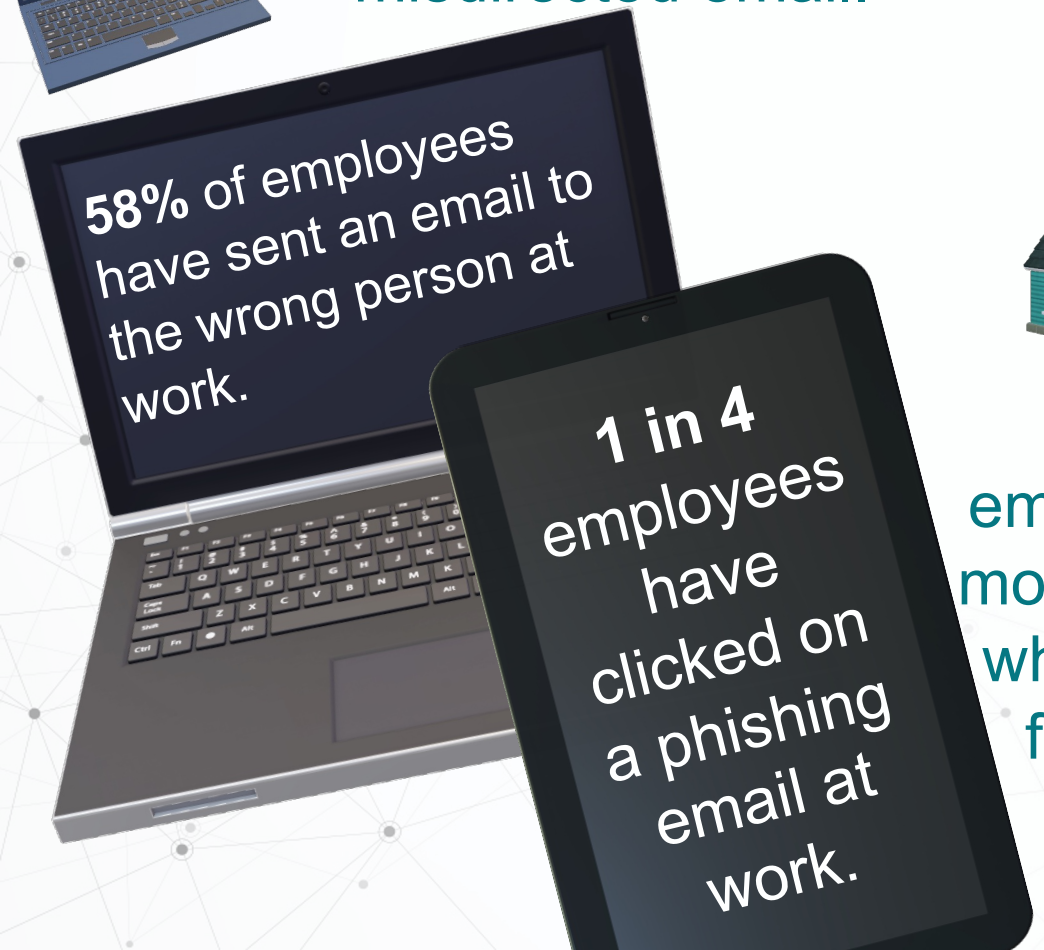
Setting the Scene

1 in 5 companies lost customers following a misdirected email.

1/3 of employees rarely or never think about cyber security at work



Younger workers are **5x** more likely to make mistakes with security consequences.



57% of employees are more distracted when working from home

93% of staff are tired and stressed at work.

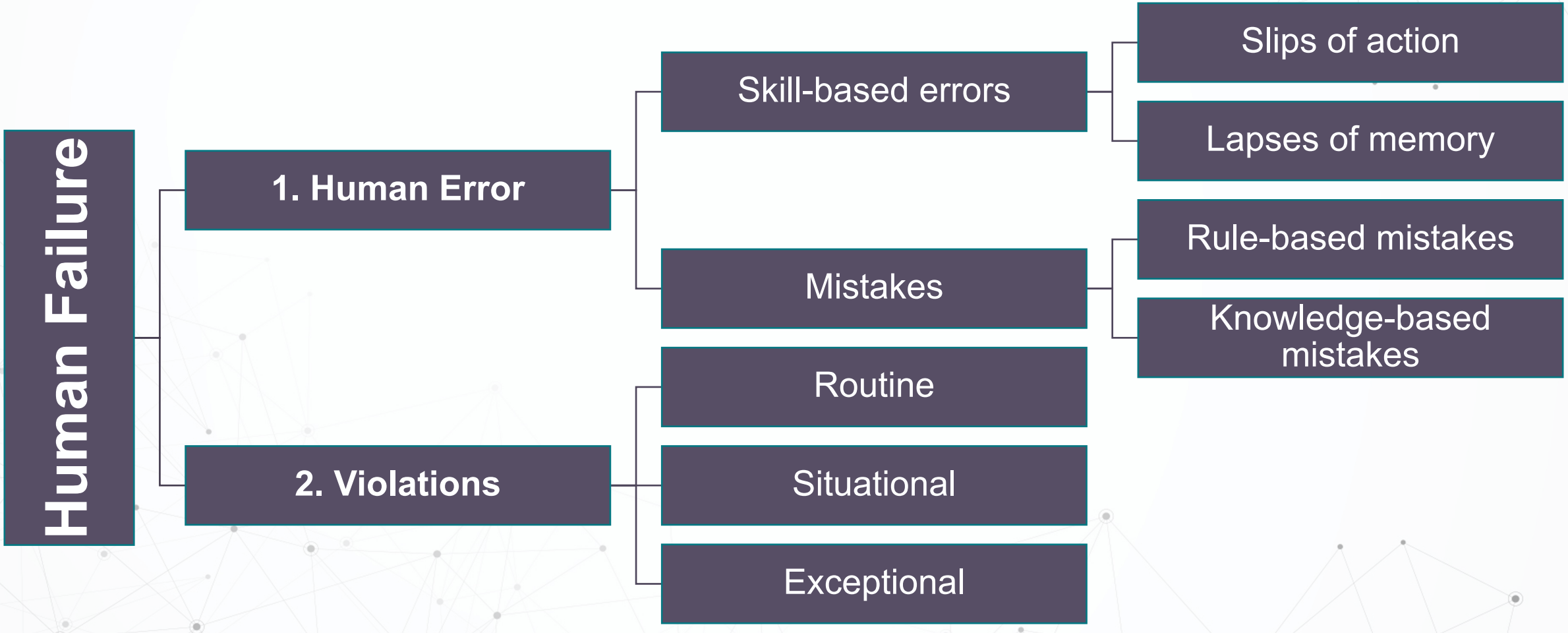
> 50% employees make more mistakes when they're stressed, while **43%** are more error-prone when tired.

1 in 10 feel tired every day of the week.

Source: The Psychology of Human Error

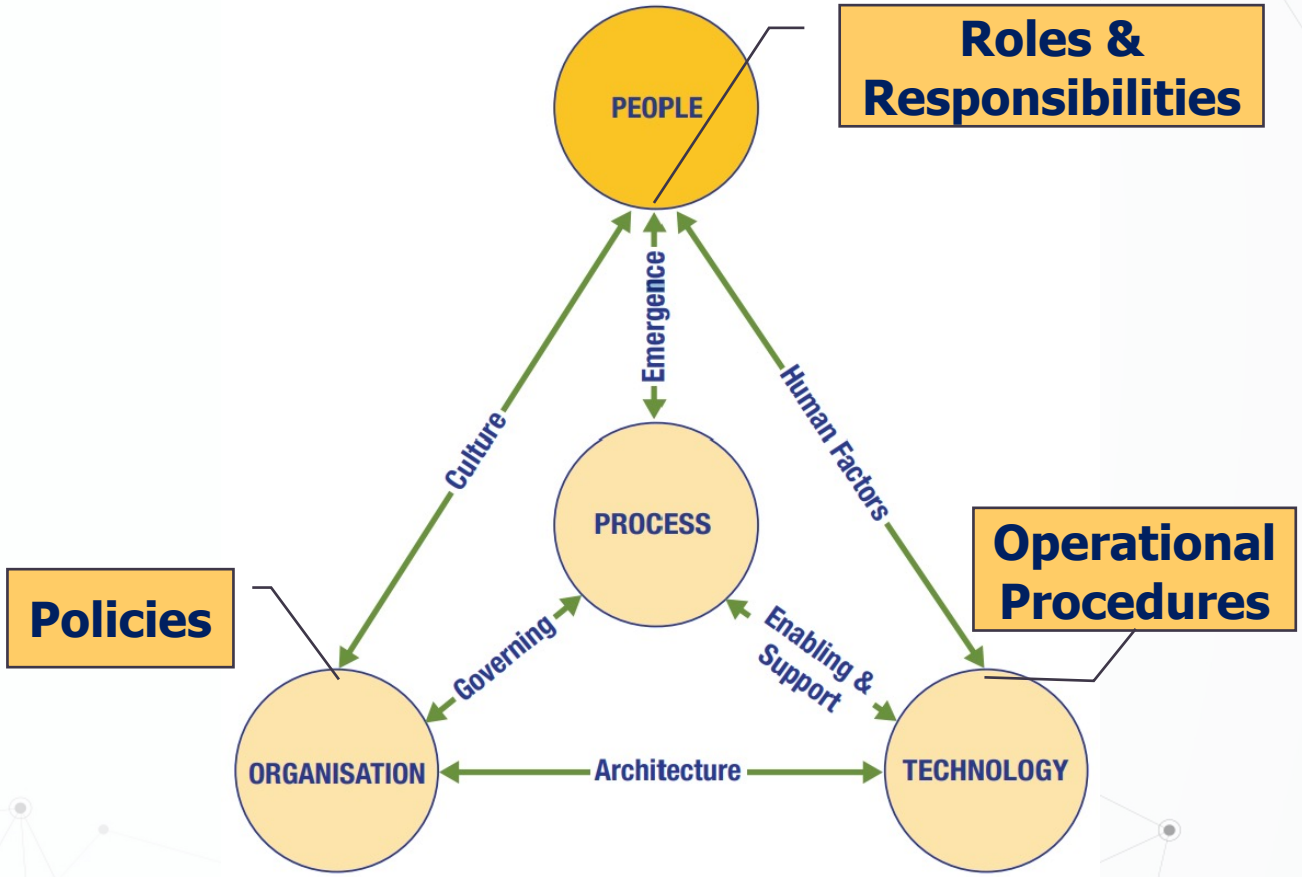
Understand the mistakes that compromise your Company's cybersecurity

Understanding Human Failure



Focus on the Human Factor

- **Policy**
  - Communicate an organization's values, philosophy, and culture.
- **Process**
  - A series of related tasks or methods that together turn inputs into outputs.
- **Operational Procedure**
  - Step-by-step instructions for specific routine tasks.



Less Is More

…

The average attention span = **8.25 seconds**

An office worker will check their email inbox, on average, **11 times an hour**.

The average person picks up their phone more than **1,500 times every week**.

Users will read **28%** of the words during an average visit of a web page

The average amount of time someone watches an internet video is **2.7 minutes**.

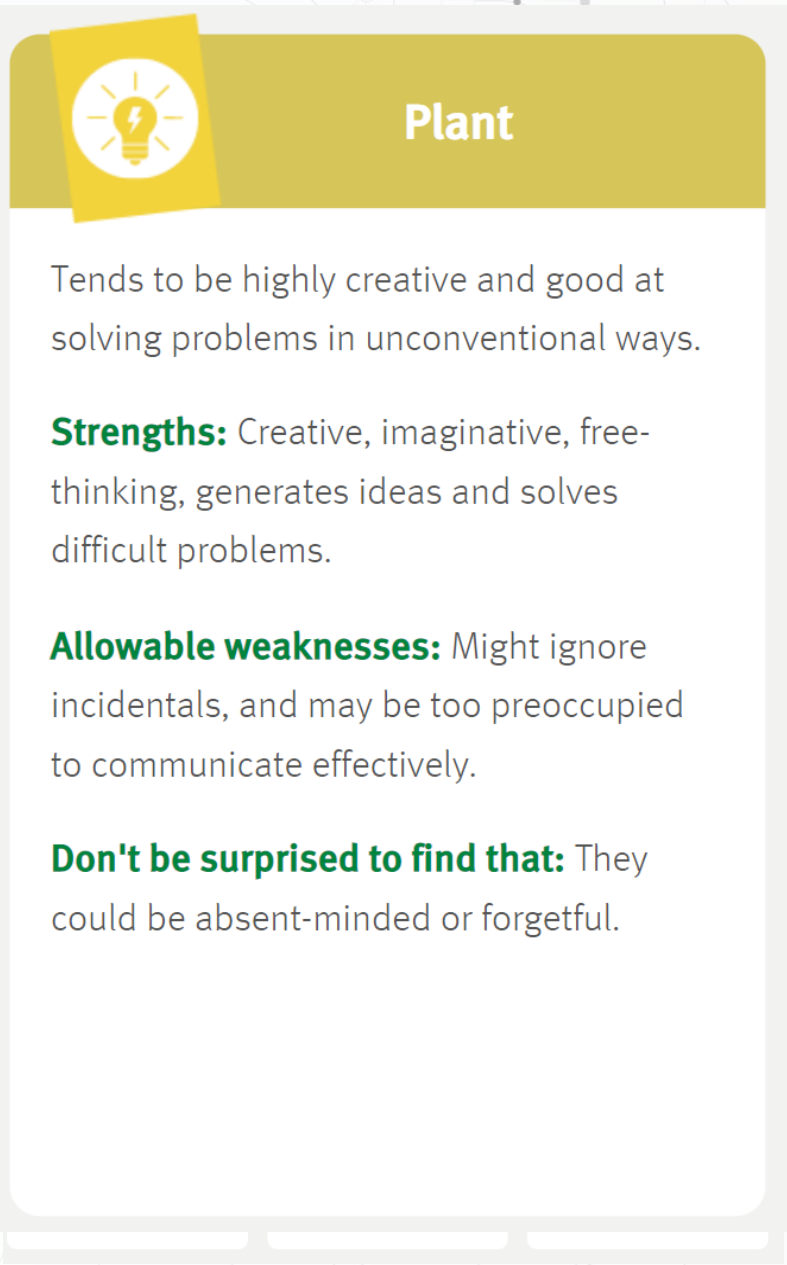
A 20-page policy will take on average **40 mins** for the employee to read.

They will switch off after 4 lines of text

59% of senior executives prefer to watch a video than read text if they had the choice.

A Time For Change?

- **Leadership.**
  - Setting the right example.
  - Supporting the initiative.
- **Followership.**
- **Embrace the Hierarchy of needs.**
  - Let them feel part of the process.
  - Welcome their contribution/support.
- **Teamwork.**
  - Know your team strengths & weaknesses
- **Work Smarter, Not Harder.**
  - Consider automation.



Engage & Explain

Think Beyond Compliance

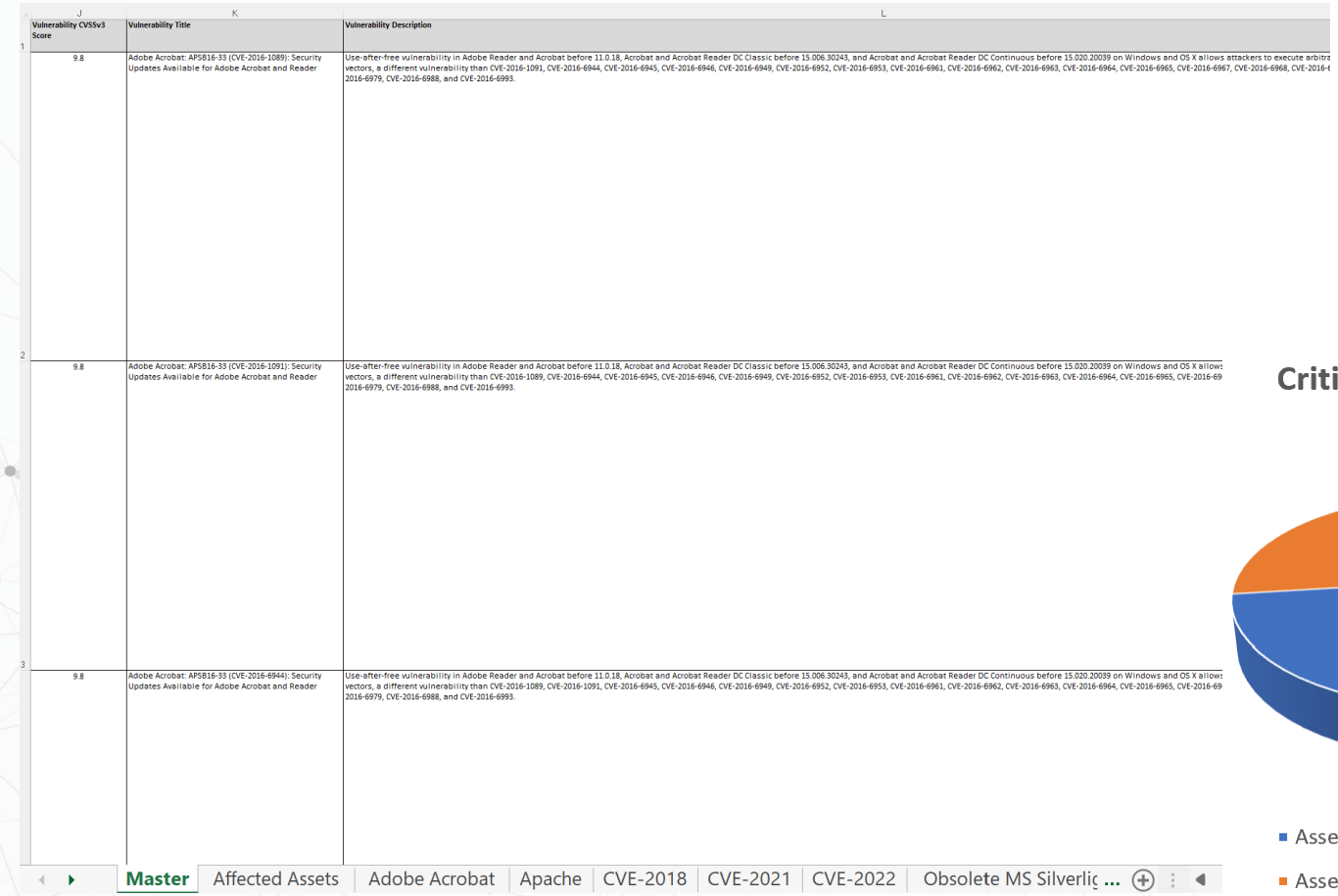
- Could you reduce the effort needed to retain secure operations?
- Do you have any single points of failure?
- Do you employ a team approach?
  - *Leadership?*
  - *Management?*
  - *Followership?*
- Do you use a variety of different ways to communicate?
- Do you use the Keep It Simple Solution (KISS)?
- Are your policies, processes & operational procedures effective?
  - *Overly wordy?*

Turning Information Into Actionable Intelligence

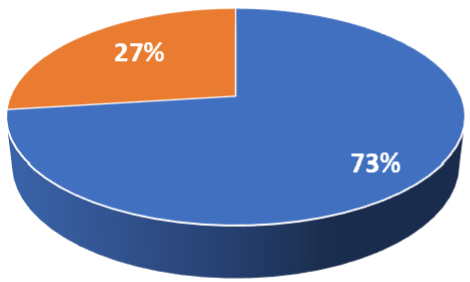
Vulnerability Management

Assets		Vulnerability Category	Count
Total Scope	55	Adobe	212
Affected assets	40	Apache	6
		MS CVE-2018	1
		MS CVE-2021	9
		MS CVE-2022	12
		Obsolete MS Silverlight	1
		McAfee Agent	1
		Totals	**242**

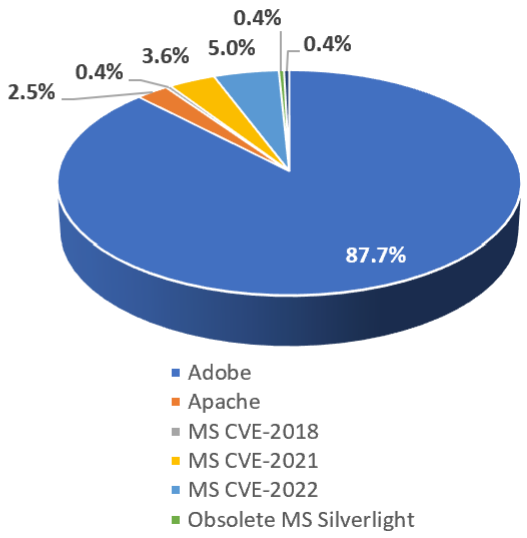
* Adobe Acrobat DC >= 15.0.20000 and < 15.020.20039 on Microsoft Windows



Critical Vulnerabilties %



Vulnerability Categories



Cybersecurity Stats & Facts

1. The worldwide information security market is forecast to reach **$366.1 billion** in 2028. (Fortune Business Insights).
2. **68%** of business leaders feel their cybersecurity risks are increasing. (Accenture).
3. On average, only **5%** of companies' folders are properly protected. (Varonis).
4. **54%** of companies say their IT departments are not sophisticated enough to handle advanced cyberattacks. (Sophos).
5. Cyber fatigue, or apathy to proactively defending against cyberattacks, affects as much as **42%** of companies. (Cisco).
6. **43%** of all breaches are insider threats, either intentional or unintentional. (Check Point).
7. Data breaches exposed **22 billion records in 2021**. (RiskBased Security).

Bibliography

- aczechowski. "What Is Configuration Manager? - Configuration Manager." *Docs.microsoft.com*, 27 June 2022, docs.microsoft.com/en-us/mem/configmgr/core/understand/introduction.
- Asana. "Team Charter Template: A Roadmap for Team Success • Asana." *Asana*, 1 Apr. 2022, asana.com/resources/team-charter-template. Accessed 11 Aug. 2022.
- ---. "What Is Management by Objectives (MBO)? Steps, Pros, and Cons • Asana." *Asana*, 7 Oct. 2021, asana.com/resources/management-by-objectives. Accessed 11 Aug. 2022.
- Belbin. "Belbin Team Roles." *Belbin*, www.belbin.com, 2022, www.belbin.com/about/belbin-team-roles. Accessed 16 July 2022.
- Brown, Rita Mae. *Sudden Death*. Toronto ; New York, Bantam Books, 1983.
- Butler, Beau. "Quasar PCI DSS Cardholder Data Discovery." *Quasar*, 2022, quasarscan.com.
- Center for Internet Security (CIS). "CIS Securesuite Build Kit Content." *CIS*, 2022, www.cisecurity.org/cis-securesuite/cis-securesuite-build-kit-content. Accessed 17 July 2022.
- Centre for Internet Security (CIS). "CIS-CAT Pro." *CIS*, 2022, www.cisecurity.org/cybersecurity-tools/cis-cat-pro. Accessed 17 July 2022.
- Cisco. "Cisco DNA Center Network Management and Automation." *Cisco*, 2022, www.cisco.com/site/us/en/products/networking/dna-center-platform/index.html.
- communications@manageengine.com, ManageEngine. "Switch Port & IP Address Management Software by ManageEngine OpUtils." *ManageEngine OpUtils*, 2022, www.manageengine.com/products/oputils/rogue-detection-and-prevention.html.
- Cooper, Stephen. "What Is a Next-Gen SIEM?" *Comparitech*, 23 May 2021, www.comparitech.com/net-admin/what-is-a-next-gen-siem. Accessed 17 July 2022.
- Cybersecurity & Infrastructure Security Agency (CISA). *AUGUST 2020 Federal Partnership for Interoperable Communications SAFECOM/National Council of Statewide Interoperability Coordinators OPERATIONAL BEST PRACTICES for ENCRYPTION KEY MANAGEMENT*. Aug. 2020.
- ExtraHop. "ExtraHop: Cloud-Native Cybersecurity Solutions | ExtraHop." *Www.extrahop.com*, 2022, www.extrahop.com. Accessed 17 July 2022.
- Gartner Digital Markets. "Proxyclick | Visitor Management Software." *Info.gartnerdigitalmarkets.com*, 2022, info.gartnerdigitalmarkets.com/proxyclick-gdm-lp/?category=visitor-management. Accessed 17 July 2022.
- GoCardless. "Management by Objectives Explained." *Gocardless.com*, Oct. 2021, gocardless.com/en-au/guides/posts/management-by-objectives-explained. Accessed 11 Aug. 2022.
- Hackr.io. "10 Best Automation Testing Tools in 2022 [Updated]." *Hackr.io*, 2022, hackr.io/blog/automation-testing-tools. Accessed 17 July 2022.
- Health & Safety Executive (HSE). *Leadership and Worker Involvement Toolkit Understanding Human Failure*.
- Inc, Gartner. "Endpoint Security and Protection Software Reviews 2021 | Gartner Peer Insights." *Gartner*, 2022, www.gartner.com/reviews/market/endpoint-protection-platforms. Accessed 17 July 2022.
- ---. "FortiGate: Next Generation Firewall (NGFW) Reviews, Ratings, and Features - Gartner 2021." *Gartner*, 2022, www.gartner.com/reviews/market/network-firewalls/vendor/fortinet/product/fortigate-next-generation-firewall-ngfw. Accessed 17 July 2022.
- Indeed Editorial Team. "What Is Followership? 10 Qualities of Supportive Followers." *Indeed Career Guide*, 14 Mar. 2022, www.indeed.com/career-advice/career-development/followership. Accessed 17 July 2022.
- Kojic, Marija. "The Most Common Workplace Distractions and Tips on How to Tackle Them." *Clockify Blog*, 9 June 2022, clockify.me/blog/productivity/workplace-distractions. Accessed 16 July 2022.
- Lindberg, Erik. *Effects of Management by Objectives Studies of Swedish Upper Secondary Schools and the Influence of Role Stress and Self-Efficacy on School Leaders*. 2011.

Bibliography

- McLeod, Saul. "Maslow's Hierarchy of Needs." *Simply Psychology*, 2022, www.simplypsychology.org/maslow.html. Accessed 16 July 2022.
- Murphy, Aislinn. "FACT CHECK: Did Albert Einstein Coin This Saying on the "Definition of Insanity"?" *Checkyourfact.com*, 26 June 2019, checkyourfact.com/2019/06/26/fact-check-albert-einstein-definition-instanity-same-thing-over-different-results. Accessed 16 July 2022.
- Nucleus. "Unified Vulnerability Management | Application Security." *Nucleus Security*, 2022, nucleussec.com. Accessed 17 July 2022.
- Omni Calculator. "Words per Minute Calculator - Speech and Reading." *Www.omnicalculator.com*, 2022, www.omnicalculator.com/everyday-life/words-per-minute. Accessed 16 July 2022.
- Park, Todd. "It's Okay to Make Mistakes." *Www.youtube.com*, 15 May 2020, youtu.be/lVnTh1RZyIY. Accessed 2 Aug. 2022.
- PermaFrostTV. "Perturbator - Humans Are Such Easy Prey. Terminator 1." *Www.youtube.com*, 3 Sept. 2015, youtu.be/T2AHGXsfV_Y. Accessed 16 July 2022.
- PowerDMS. "What Is a Policy vs. a Procedure?" *Www.powerdms.com*, 22 Dec. 2020, www.powerdms.com/policy-learning-center/what-is-a-policy-vs.-a-procedure. Accessed 16 July 2022.
- Practical Psychology. "False Memories and Memory Errors | Practical Psychology." *Practical Psychology*, 29 July 2019, practicalpie.com/false-memories-and-memory-errors. Accessed 16 July 2022.
- Rolf Von Roessing, and Information Systems Audit And Control Association. *The Business Model for Information Security*. Meadows, Ill., Isaca, 2010.
- SecTools.org. "SecTools.org Top Network Security Tools." *Sectools.org*, 2022, sectools.org.
- Sobers, Rob. "110 Must-Know Cybersecurity Statistics for 2020 | Varonis." *Inside out Security*, 20 Nov. 2019, www.varonis.com/blog/cybersecurity-statistics. Accessed 16 July 2022.
- SolarWinds. "Network Mapping Software | SolarWinds." *Solarwinds.com*, 2016, www.solarwinds.com/network-topology-mapper. Accessed 17 July 2022.
- SourceForge. "Best Website Security Software - 2022 Reviews & Comparison." *Sourceforge.net*, 2022, sourceforge.net/software/website-security/. Accessed 17 July 2022.
- Tallyfy. "Process vs Procedure: What's the Difference?" *Tallyfy*, 23 Jan. 2018, tallyfy.com/procedure-vs-process. Accessed 16 July 2022.
- Tessian. "Psychology of Human Error 2022 | Research Report." *Tessian*, 2022, www.tessian.com/resources/psychology-of-human-error-2022. Accessed 16 July 2022.
- Titania. "How to Audit for PCI DSS Using Nipper - Titania." *Titania.com*, 2022, www.titania.com/resources/nipper/how-to-audit-for-pci-dss-using-nipper/. Accessed 17 July 2022.
- Trend Micro. "Advanced XDR Capabilities - Now with Vision One." *Trend Micro*, 2022, www.trendmicro.com/en_us/business/products/detection-response/xdr.html. Accessed 17 July 2022.
- Webteam, Puppet. "Configuration Management with Puppet - IT Automation for Everyone." *Puppet.com*, 2022, puppet.com/use-cases/continuous-configuration-automation. Accessed 17 July 2022.
- Wireshark Foundation. "Wireshark." *Wireshark.org*, 2016, www.wireshark.org/.
- world economic forum. "Global Risks Report 2022." *World Economic Forum*, 11 Jan. 2022, www.weforum.org/reports/global-risks-report-2022. Accessed 16 July 2022.
- Zauderer, Steven. "Average Human Attention Span by Age (Study 2022)." *Www.crossrivertherapy.com*, 11 July 2022, www.crossrivertherapy.com/average-human-attention-span.
- Zelleke, Liku. "7 Best Automated Patch Management Tools for 2022 (Paid & Free)." *Comparitech*, 2 July 2021, www.comparitech.com/net-admin/best-automated-patch-management-tools. Accessed 17 July 2022.
- Zortrex. "Token Vault." *Zortrex*, 2022, zortrex.com/token-vault. Accessed 17 July 2022.