THE TOP 10 CYBER SECURITY SKILLS YOU NEED TO MASTER – NOW

MATTHEW FREDERICKSON

SOME STATISTICS

- Security attacks increased 31% from 2020 to 2021, according to Accenture's "State of Cybersecurity Resilience 2021" report. The number of attacks per company increased from 206 to 270 year over year.
- It takes an average of 287 days for security teams to identify and contain a data breach, according to the "Cost of a Data Breach 2021" report released by IBM and Ponemon Institute.
- The FBI's Internet Crime Complaint Center (IC3) reported an all-time high volume of complaints in 2020 at 791,790. Total losses from those complaints was more than $4.1 billion.
- Phishing, the most common threat vector, is involved in 36% of data breaches, according to Verizon's "2021 Data Breach Investigations" report.
- According to Emsisoft's "The State of Ransomware in the US" report, an estimated 2,323 local governments, schools and healthcare providers were directly affected as victims of a ransomware attack in 2021.

SOME STATISTICS

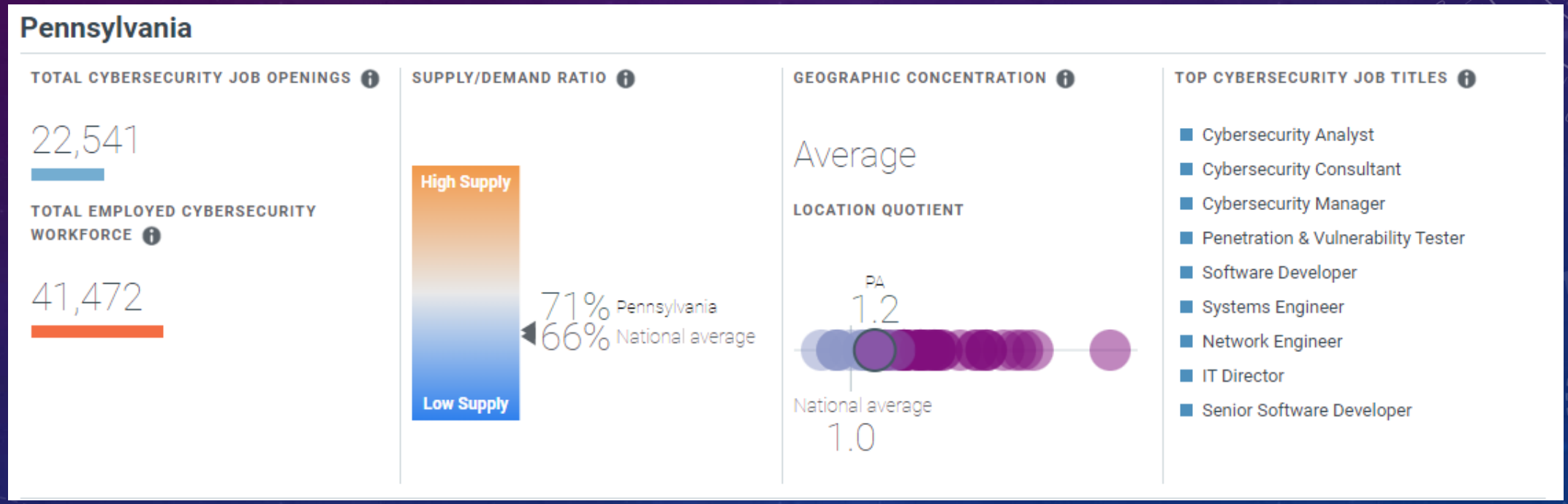
- More than **90%** of cyber attacks begin as spear phishing emails, according to Trend Micro researchers.
- A single attack -- be it a data breach, malware, ransomware or DDoS attack -- costs companies of all sizes an average of $200,000, and many affected companies go out of business within six months of the attack, according to insurance company Hiscox.
- Forty-three percent of attacks are aimed at SMBs, but only 14% are prepared to defend themselves, according to Accenture.
- At the end of 2021, there was a security workforce gap of 377,000 jobs in the U.S and 2.7 million globally, according to the "(ISC)2 Cybersecurity Workforce Study, 2021."
- The "ISACA State of Cybersecurity 2021 Part 1" survey states that 61% of organizations feel they are understaffed in terms of cybersecurity professionals. Fifty percent of respondents said applicants were not sufficiently qualified for security positions.

SOME STATISTICS

- The study also found that only 27% of recent graduates in cybersecurity education programs are properly prepared for the workforce.

- Cybersecurity is a high-salary field to work in, particularly in North America. The "(ISC)2 Cybersecurity Workforce 2021" study stated that the average salary for a cybersecurity professional in North America was **$119,898**. That figure drops to $78,618 in Europe and falls even further in Latin America to $32,637.

PENNSYLVANIA



https://www.cyberseek.org/heatmap.html

PENNSYLVANIA

- Current openings requesting certifications
  - As of October 1, 2022 (https://www.cyberseek.org/heatmap.html)
- CompTIA Security+ = 4,275
- Certified Information Systems Security Professional (CISSP) = 2,898
- Global Information Assurance Certification (GIAC) = 2,226
- Certified Information Systems Auditor (CISA) = 1,524
- Certified Information Security Manager (CISM) = 519
- Certified Information Privacy Professional (CIPP) = 259

TEN SKILLS TO MASTER - TODAY

- Regardless of position, employment status, information security is YOUR responsibility
- EVERYONE who touches data – yours, or anyone else's – needs to understand the risks
- Common sense is a very powerful weapon – learn to use it
- The following 10 skills are simply my opinion. Your mileage may very
- This list is in no way complete, master these, good to go for ever…..
  - It is a journey

TOP 10 SKILLS

- Critical Thinking
- Threat Knowledge
- Controls and Frameworks
- Risk Management
- Communications
- Context
- Data-driven Conclusions
- Understanding Technology
- Understanding Identity/Access Management
- Know How Applications Work

CRITICAL THINKING

- What is critical thinking?
  - "…the ability to reason well in highly precise contexts as well as ambiguous and uncertain contexts, to ability to analyze problems and to evaluate alternatives, and the ability to explain clearly what needs to be done and why." - https://www.insightassessment.com/article/cyber-security-starts-with-critical-thinking
  - "In my opinion, the most critical skill for a cyber security professional is critical thinking — or objectively analyzing an issue to form a judgment. For me, critical thinking is about understanding the 'why' and not just the 'how' so you can make good decisions and implement solutions that address the root cause of an issue and not just the symptom." – Jill Knesek (https://www.tripwire.com/state-of-security/featured/important-skills-cyber-security-professionals/)
  - "…well cultivated critical thinker gathers and assesses relevant information and comes to well-reasoned conclusions and solutions. One also thinks open-mindedly within alternative systems of thought, while recognizing and assessing their assumptions, implications, and practical consequences." – Foundation for Critical Thinking (https://www.criticalthinking.org/pages/defining-critical-thinking/766)

CRITICAL THINKING

- Means you:
  - Ask the right questions
  - Identify your assumptions
  - Apply quantitative and algorithmic skills
  - Evaluating data for accuracy, relevance, and completeness
  - Adapt systems to the constantly changing technological environment
  - identify and integrate the latest security intelligence
  - Draw conclusions

CRITICAL THINKING

- Some questions you need to answer:
  - Why do I need to worry about information security?
  - What are the biggest threats right now?
  - How am I protecting myself against these threats?
    - Am I doing the right things?
    - Am I doing them the right way?
    - Am I getting the benefits?
  - Do I need cyber liability insurance?
  - Do I know where my data is and is it protected?
  - When did I do my last immutable backup?

THREAT KNOWLEDGE

- “Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications, and action-oriented advice about an existing or emerging menace or hazard to assets. This intelligence can be used to inform decisions regarding the subject’s response to that menace or hazard.” – Gartner

- “Threat intelligence is the analysis of data using tools and techniques to generate meaningful information about existing or emerging threats targeting the organization that helps mitigate risks.” – EC Council

- “Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor’s motives, targets, and attack behaviors. Threat intelligence enables us to make faster, more informed, data-backed security decisions and change their behavior from reactive to proactive in the fight against threat actors.” - Crowdstrike

THREAT KNOWLEDGE

- It’s as simple as Who, What, When, Where, Why and How
  - Who presents the risk?
  - What are they trying to get?
  - When will they attack?
  - Where are they coming from, and where are they attacking?
  - Why are you a target?
  - How are they going to do it?

THREAT KNOWLEDGE

- Where to go?
  - AlienVault Open Threat Exchange (https://otx.alienvault.com)
  - Cisco Talos Intelligence (https://www.talosintelligence.com/)
  - The Spamhaus Project (https://www.spamhaus.org/)
  - Department of Homeland Security (DHS): CISA Automated Indicator Sharing (https://www.cisa.gov/ais)
  - SANS Internet Storm Center (https://isc.sans.edu/)
  - VirusTotal (https://www.virustotal.com/gui/home/upload)
- Google is your friend

CONTROLS AND FRAMEWORKS

- “Cybersecurity controls are **mechanisms used to prevent, detect and mitigate cyber threats and attacks**. Mechanisms range from physical controls, such as security guards and surveillance cameras, to technical controls, including firewalls and multifactor authentication.” – Tech Target

- “Cybersecurity controls are the processes your organization has in place to protect from dangerous network vulnerabilities and data hacks. The cybersecurity controls organizations use are meant to detect and manage the threats to network data. There will always be new threats and vulnerabilities as technology evolves, but controls are set in place to reduce the overall threat of exposure.” – BitSight

- “Security controls are parameters implemented to protect various forms of data and infrastructure important to an organization. Any type of safeguard or countermeasure used to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets is considered a security control.” - IBM

CONTROLS AND FRAMEWORKS

- “…a cybersecurity framework provides a set of "best practices" for measuring risk tolerance and establishing controls…” – PreyProject.com

- “A cybersecurity framework provides a common language and set of standards for security leaders across countries and industries to understand their security postures and those of their vendors. With a framework in place it becomes much easier to define the processes and procedures that your organization must take to assess, monitor, and mitigate cybersecurity risk.” – BitSight

- “Cyber security frameworks are sets of documents describing guidelines, standards, and best practices designed for cyber security risk management. The frameworks exist to reduce an organization's exposure to weaknesses and vulnerabilities that hackers and other cyber criminals may exploit.” - Simplilearn

CONTROLS AND FRAMEWORKS

- Controls provide a way to measure
  - “I often say that when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science, whatever the matter may be.” – William Thomson, Lord Kelvin

- Frameworks provide ***guidance*** on what controls to use and WHY you should consider using them

- Consistency is the main goal – to understand abnormal you have to understand normal

CONTROLS AND FRAMEWORKS

- NIST Cybersecurity Framework (CSF) (https://www.nist.gov/cyberframework)
- CIS Critical Security Controls (https://www.cisecurity.org/controls/cis-controls-list)
- Australian Cyber Security Essential Eight Maturity Model (https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model)
- Cloud Security Alliance Cloud Controls Matrix (https://cloudsecurityalliance.org/research/cloud-controls-matrix/)
- Control Objectives for Information Technology (COBIT) (https://www.isaca.org/resources/cobit)
- Cybersecurity Maturity Model Certification (CMMC) (https://www.acq.osd.mil/cmmc/)
- European Union Agency for Cybersecurity (ENISA) National Capabilities Assessment Framework (https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework)

CONTROLS AND FRAMEWORKS

- Factor Analysis of Information Risk (FAIR) Cyber Risk Framework (https://www.fairinstitute.org/)
- HITRUST CSF Framework (https://hitrustalliance.net/product-tool/hitrust-csf/)
- Information Security Forum (ISF) Standard of Good Practice for Information Security (SOGP 2020) (https://www.securityforum.org/solutions-and-insights/standard-of-good-practice-for-information-security-2020/)
- International Office of Standardization (ISO) 27001 (https://www.iso.org/isoiec-27001-information-security.html)
- National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) (https://www.ncsc.gov.uk/collection/caf)

RISK MANAGEMENT

- “Cyber risk management means identifying, analysing, evaluating and addressing your organisation's cyber security threats. The first part of the cyber security risk management process is a cyber risk assessment.” – ITGovernance.co.uk

- “Cybersecurity Risk Management must be continuous in order to maintain protections.” – Rapid7

- “Cybersecurity risk management is the practice of prioritizing cybersecurity defensive measures based on the potential adverse impact of the threats they're designed to address.” – AT&T

RISK MANAGEMENT

- Step 1 – Identify what's important
- Step 2 – Identify how it is accessed, stored, changed, deleted
- Step 3 – Identify your threats – WHO might want access to you and/or your data
  - Why? What is their benefit?
- Step 4 – Identify what CONTROLS you have in place to keep things safe
- Step 5 – Calculate the COST of prevention vs the COST of what's being protected
  - This sets the hierarchy
- Step 6 - Repeat

RISK MANAGEMENT

- NIST Risk Management Framework (RMF) (https://csrc.nist.gov/projects/risk-management/about-rmf)
- International Office of Standardization (ISO) 27001 (https://www.iso.org/isoiec-27001-information-security.html)
- Factor Analysis of Information Risk (FAIR) Cyber Risk Framework (https://www.fairinstitute.org/)

COMMUNICATIONS

- “The imparting or exchanging of information or news.” – Oxford Dictionary
- “The Cybersecurity and Communications Reliability Division (CCR) helps ensure that the nation’s communications networks are reliable and secure so that the public can communicate, especially during emergencies.” – FCC
- “This means **communicating with all your audiences**, which will likely include your customers, internal staff, regulators, lawmakers, and the media.” – Tucker/Hall

COMMUNICATIONS

- FCC Cyberplanner (https://www.fcc.gov/cyberplanner)
- Developing an Effective Cybersecurity Communication Plan (https://blog.investorrelations.com/blog/developing-an-effective-cybersecurity-communication-plan)
- Creating a Communications Plan (Workbook) (https://www.wallacefoundation.org/knowledge-center/Documents/Workbook-A-Communication.pdf)

COMMUNICATIONS

- In the event of an incident
  - Know WHO you need to contact
  - Know WHO will be responsible
    - Internal
    - External
  - Know HOW you will communicate
    - Out of band
    - Email, cell phones, sneaker net
  - Know WHAT will be communicated

CONTEXT

- “The circumstances that form the setting for an event, statement, or idea, and in terms of which it can be fully understood and assessed.” – Oxford Dictionary

- “ **it is contextual information that provides insight into the circumstances of an event, and it is this insight that often determines the correct classification of a given event as an incident or – *false-positive*”** - Stinet

- “Context is about three key points: Prioritization, Urgency, and Achievability.” - Cymulate

CONTEXT

- Which item listed below is found in a rainbow (select 1):
  - Red
  - Orange
  - Blue
  - Yellow

CONTEXT

- Must be able to understand if it's an event, an incident, or an attack
- Must understand how an email can lead to a compromise
  - How to get from point A to point B
- When looking at a single data point – understand how it relates to everything else
- Ask yourself "What questions am I not asking?"

DATA-DRIVEN CONCLUSIONS

- “Things known or assumed as facts, making the basis of reasoning or calculation.” – Oxford Dictionary
- “Data based decision making provides businesses with the capabilities to generate real time insights and predictions to optimize their performance.” – Datapipe.com
- “…it's through data that you verify, understand, and quantify.” – Tim Stobierski, Harvard Business School
- “… business-based decisions should be backed by razor-sharp metrics, facts, figures, or insights related to your aims, goals, or initiatives that can ensure a stable backbone to your management reports and business operations.” - Bernardita Calzon, Business Intelligence

DATA-DRIVEN CONCLUSIONS

- Establish these core capabilities:
  - Find unbiased data sources
  - Develop analytical skills
  - Develop data-driven culture

- Critical Steps for Success
  - Define your goals
  - Identify sources of data (internal and external)
  - Determine how to collect, store, process and purge the data
  - Determine best tool for developing reports and/or delivering analysis
  - Plan, Do, Study, Act

DATA-DRIVEN CONCLUSIONS

- Needs an acronym – Data-driven Decision Making (DDDM)

- Things to avoid:
  - Bad data
  - Weak Analysis
  - Bad Interpretation
  - Wrong Decisions
  - Faulty Execution
  - No Learning

UNDERSTANDING TECHNOLOGY

- “Technology is the application of scientific knowledge to the practical aims of human life or, as it is sometimes phrased, to the change and manipulation of the human environment.” – Britannica

- ‘Information Technology means the use of hardware, software, services, and supporting infrastructure to manage and deliver information using voice, data, and video.” – ND Century Code (Chapter 54.59.01)

- There are three primary pillars of responsibility for an IT department:
  - IT governance
  - IT operations
  - Hardware and infrastructure

UNDERSTANDING TECHNOLOGY

- What you need to know:
  - How a computer works (think CompTIA A+)
  - How computers talk to each other – networking (think CompTIA Network+)
  - How to protect those resources (think CompTIA Security+)

- What you don’t need to know
  - How to create a circuit board
  - How to build a router

UNDERSTANDING TECHNOLOGY

- Ask yourself these questions:
  - Do you understand how email works?
  - Do you understand where files are stored on your computer?
  - Do you know what normal traffic looks like on your network?
  - Do you know how to spot abnormal behavior?
  - Are you running a behavioral based anti-virus/malware tool on your desktops?
  - Do you have backups, immutable, of what's important?

UNDERSTANDING IDENTITY/ACCESS MANAGEMENT

- “Identity management is all about managing the attributes related to the user, group of users, or other identity that may require access from time to time.” – Vmware

- “Identity management and access control is the discipline of managing access to enterprise resources to keep systems and data secure.” – Okta

- “Identity management (ID management) is the organizational process for ensuring individuals have the appropriate access to technology resources.” – TechTarget.com

UNDERSTANDING IDENTITY/ACCESS MANAGEMENT

- Understand the following:
  - MFA – Multi-factor Authentication
  - SSO - Single Sign-on
  - OIDC – OpenID Connect
  - ADFS – Active Directory Federated Service
  - LDAP – Lightweight Directory Access Protocol
  - Federation - Identity federation is a system of trust between two parties for the purpose of authenticating users and conveying information needed to authorize their access to resources.
  - Kerberos – network authentication protocol

UNDERSTANDING IDENTITY/ACCESS MANAGEMENT

- What you should be doing:
  - Never log onto computer with admin level
    - This means whatever account you used to setup Windows – create a user account to use day by day
  - Use a secure password phrase
  - Different passwords for EVERY web site/service you use
  - KNOW what to do in the event your have been compromised
    - It’s not if but when

UNDERSTANDING IDENTITY/ACCESS MANAGEMENT

- Some Best Practices:
  - Adopt a Zero Trust Approach to Security
  - Identify and Protect High-Value Data
  - Enforce a Strong Password Policy
  - Use Multi-Factor Authentication (MFA)
  - Automate Workflows
  - Adopt The Principle of Least Privilege
  - Enforce Just-in-Time Access Where Appropriate

KNOW HOW APPLICATIONS WORK

- A program or piece of software designed and written to fulfill a particular purpose of the user.” – Oxford Dictionary

- “An application, also referred to as an application program or application software, is a computer software package that performs a specific function directly for an end user or, in some cases, for another application. An application can be self-contained or a group of programs. The program is a set of operations that runs the application for the user.” – Alexander S. Gillis, TechTarget.com

KNOW HOW APPLICATIONS WORK

- There are three main types of programs/applications:
  - Desktop
  - Web based
  - Mobile (apps)

- Understand EVERY program has a purpose
  - Usually takes data in
  - Does something to the data
  - Spits something out/performs some action

KNOW HOW APPLICATIONS WORK

- #1 issue with applications
  - Input validation
- #2 issue with applications
  - Input validation
- #3 issue with applications
  - Programmers not putting security first (DevOps)
- #4 issue with applications
  - Input validation
  - Seriously – has been an issue for over 20 years

KNOW HOW APPLICATIONS WORK

- What YOU need to know:
  - Know what's running on your desktop, your phone, your network
  - Know who has access to what – and why (think RBAC)
  - Know who has the ability to grant/revoke access
- Before you use an app
  - Make sure you know where it came from
  - Make sure you know what it's doing
    - i.e. search for something on Amazon and an ad appears for the exact same thing on a different web site
    - There is no such thing as a coincident

QUESTIONS?

MATT FREDERICKSON

MFREDERICKSON@CRSD.ORG