Tom Scott

Cyber Resilience Professional

Certified Information Systems Security Professional
Certified Information Systems Auditor
Certified Risk Information Systems Control
Project Management Professional
Certified Critical Infrastructure Manager
Stacey Coleman

Stacey is a 28-year law enforcement officer currently employed with the Solicitors Office of the 2nd Judicial Circuit. He is the program coordinator for a fraud division and serves as the agency's security officer. He started his own IT Company in 1999 and provides managed services to a number of small business. He is the founder of POISN (Police Officer Information Security Network) which provides training and technical assistance to agencies governed by Criminal Justice Information Security Policy (CJIS). Additionally, he serves as a government facilities sector chief with Infragard and holds a Master Degree in Human Relations from Liberty University.
What is Cybersecurity?

Definition of Cybersecurity

*noun:* measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack

Simply put, cybersecurity is protection against digital attacks.

The Department of Homeland Security says it best: “Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace.”
Why is Cybersecurity so important?
'Why are you looking at me? I see you watching me.' Smart devices like Nest getting hacked in digital home invasions.

'Why are you looking at me? I see you watching me.' Smart devices like Nest getting hacked in digital home invasions.

Why is Cybersecurity so important?
What’s the big deal about Cybersecurity?

• By 2021, cybercrimes will cost $6 trillion per year worldwide

• The cost of cybercrimes will double in the next five years, up from $3 trillion in 2015, according to a report Cybersecurity Ventures.

• This includes not only stolen money and ransom, but also the value of lost productivity and intellectual property, data theft, business disruption, reputational harm and more.
What’s the big deal about Cybersecurity?

- Businesses experience ransomware attacks every 14 seconds

- According to Kaspersky Lab, businesses experience a ransomware attack every 14 seconds in 2019 up from every 2 minutes just several years ago. This is expected to increase to every 11 seconds by 2021.

- Currently, there are more than 4,000 ransomware attacks every day. - FBI
Alabama County Offices Work to Reopen After Cyberattack

Chilton County, Ala., officials say that they hope to reopen a pair of governmental office services during the week to come after a nearly two-week closure that was caused by a ransomware attack.

BY ANNA BEAHM, ALABAMA MEDIA GROUP / JULY 20, 2020
What’s the big deal about Cybersecurity?

• Email is the number #1 delivery vehicle for most malware and ransomware.

• Verizon reports that users in the U.S open 30 percent of phishing all emails, with 12 percent of those targeted by these emails clicking on the infected links or attachments.

• Spear phishing accounts for 91% of attacks!
I should warn you all I might have just clicked on a link that means we should immediately seek alternative employment.
What’s the big deal about Cybersecurity?

This is potentially because they are the most technologically savvy group. In any case, around **53 percent** of millennials experienced cyber crime in the last year.
What’s the big deal about Cybersecurity?

• Since 2013 there are 3,809,448 records stolen from breaches every day.

• That’s 158,727 per hour, 2,645 per minute and 44 every second of every day reports Cybersecurity Ventures.
“...what we have to remember is those who attack are patient, and those that attack never stop trying.

So, if that’s the case, we can never stop working to make sure we keep things safe.”

-- Governor Nikki Haley
City of Atlanta Incident

Headline: “Atlanta is being held hostage by hackers”.

The Georgia capital with 8,000 employees was subject to a ransomware attack by the mysterious SamSam hacking crew on March 21, 2018. While city employees were finally able to use their computers on March 27th, police officers were still writing by hand, and city courts are closed. Residents can’t pay bills online or use Wi-Fi at the airport.

Attackers demanded $51,000 worth of bitcoin. “We are dealing with a hostage situation,” said Mayor Keisha Lance Bottoms.

What’s the big deal about Cybersecurity?
What’s the big deal about

Louisiana Governor Declares State of Emergency After Ransomware Hits School Systems

Parishes of Oachita, Morehouse and Sabine. Phone systems were reportedly also disrupted.

1. Consider each asset’s value and vulnerability.
2. Train and motivate all workers.
3. Scan for vulnerabilities frequently.
4. Establish appropriate goals and metrics.

Georgia State Patrol working on computer fix after cyber attack

Three months after hackers struck, the Georgia Department of Public Safety has 50 workers trying to mitigate the damage to its computer system and regain access to records.

By Joshua Sharpe, The Atlanta Journal-Constitution
What's the big deal about Cybersecurity?

- 23 Texas Cities

- August, 2019 - Cybersecurity experts have been deployed by the state to assess the damage from a "coordinated ransomware attack" that struck 23 Texas cities on Friday, state officials said.

- Texas Gov. Greg Abbott ordered a "Level 2 Escalated Response" to the attacks, one step below the Texas Division of Emergency Management's highest level of alert. The designation means the emergency is beyond the scope of local responders.
What’s the big deal about Cybersecurity?

Closer to home...

In 2012 SC suffered one of the largest state level breaches in US history when the Department of Revenue was hit.

- 3.6 million taxpayer social security numbers
- 1.9 million dependent social security numbers
- 3.3 million credit card/bank accounts
What’s the big deal about Cybersecurity?

Closer to home…

- According the FBI, approximately $900,000 was stolen via bank robberies in South Carolina during 2017.

- During that same period, closer to $6 million was stolen via business email compromise (BEC) in South Carolina.

- Nationwide, the FBI claims that BEC scams have accounted for $5 billion in losses between from Oct 2013 to Dec 2016.
What’s the big deal about Cybersecurity?

Closer to home…

- Dorchester School District 2 paid a ransom in 2017, as did Horry County Schools a year earlier. As is typical in ransomware attacks, the disruption was great but relatively small ransoms were demanded — $2,900 for Dorchester 2, $8,500 for Horry — to be paid with the electronic currency Bitcoin.

- “We had no choice if we wanted the data returned in a reasonable period of time,” Charles Hucks, then-Horry County Schools executive director of technology, stated at a hearing of the Senate Judiciary.
What can you do?

Be cybersecurity advocates at your organization.

Constantly train your employees.

Have good endpoint solutions.

Ensure you’re backing up your vital systems.

Trust but verify.

ESSENTIAL ELEMENT: YOURSELF, THE LEADER

THE TASK: Drive Cybersecurity Strategy, Investment and Culture

Being a cyber leader does not require technical expertise, but rather an ability to change the culture of your organization. Reducing your organization's cyber risks requires awareness of cybersecurity basics. As a leader, you need to drive your organization's approach to cybersecurity as you would any other hazard (e.g. how you identify risk, reduce vulnerabilities, and plan for contingencies). This requires an investment of time and money, as well as the collective buy-in of your management team. Your investment drives actions and activities, and these build and sustain a culture of cybersecurity.

ESSENTIAL ELEMENT: YOURSELF, THE LEADER

Essential Actions

Approach cyber as a business risk. Ask yourself what type of impact would be catastrophic to your operations? What information if compromised or breached would cause damage to employees, customers, or business partners? What is your level of risk appetite and risk tolerance? Raising the level of awareness helps reinforce the culture of making informed decisions and understanding the level of risk to the organization.

Resources for Taking Action

National Association of Corporate Directors: The NACD Director’s Handbook on Cyber-Risk Oversight is built around five core principles that are applicable to board members of public companies, private companies, and nonprofit organizations of all sizes and in every industry sector.

National Institute of Standards and Technology (NIST) Cybersecurity Framework: Created through collaboration between industry and government, the voluntary Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure, and helps owners and operators of critical infrastructure manage cybersecurity-related risks.

CISA Security Tip – Questions Every CEO Should Ask About Cyber Risks: Provides a primer on basic questions that CEOs of all businesses should ask themselves and their employees to ensure better cybersecurity preparedness and resilience.

U.S. Small Business Administration: Small Business Cybersecurity: A guide to help leaders of small businesses learn about common cyber threats, gain an understanding about where their business might be vulnerable, and steps they can take to improve their level of cybersecurity.
ESSENTIAL ELEMENT: YOURSELF, THE LEADER

Determine how much of your organization’s operations are dependent on IT. Consider how much your organization relies on information technology to conduct business and make it a part of your culture to plan for contingencies in the event of a cyber incident. Identify and prioritize your organization’s critical assets and the associated impacts to operations if an incident were to occur. Ask the questions that are necessary to understanding your security planning, operations, and security-related goals. Develop an understanding of how long it would take to restore normal operations. Resist the “it can’t happen here” pattern of thinking. Instead, focus cyber risk discussions on “what-if” scenarios and develop an incident response plan to prepare for various cyber events and scenarios.

Resources for Taking Action

Cyber Readiness Institute: The Cyber Readiness Program is a practical, step-by-step guide to help small and medium-sized enterprises become cyber ready. Completing the Program will make your organization safer, more secure, and stronger in the face of cyber threats. The Cyber Readiness Program also provides a template for an incident response plan that your organization can customize.

CISA CRR Supplemental Resource Guide Risk Management: The principal audience for this guide includes individuals responsible for managing risk management programs for IT operations, including executives who establish policies and priorities for risk management, managers and planners who are responsible for converting executive decisions into action plans, and operations staff who implement those operational risk management plans.

NIST Small Business Cybersecurity Corner: This platform provides a range of resources chosen based on the needs of the small business community. These resources include planning guides, guides for responding to cyber incidents, and cybersecurity awareness trainings.
**ESSENTIAL ELEMENT: YOURSELF, THE LEADER**

**Lead investment in basic cybersecurity.** Invest in cybersecurity capabilities for your organization and staff. This includes not only investments in technological capabilities, but also a continuous investment in cybersecurity training and awareness capabilities for your organization’s personnel. Use the Cyber Essentials to have conversations with your staff, business partners, vendors, managed service providers, and others within your supply chain. Use risk assessments to identify and prioritize allocation of resources and cyber investment.

**Resources for Taking Action**

**NIST Cybersecurity Framework:** Created through collaboration between industry and government, the voluntary Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure, and helps owners and operators of critical infrastructure manage cybersecurity-related risk.

**Cyber Readiness Institute: The Cyber Readiness Program** is a practical, step-by-step guide to help small and medium-sized enterprises become cyber ready. Completing the Program will make your organization safer, more secure, and stronger in the face of cyber threats. The Program also provides guidance on how to select a cyber leader to create a culture of cyber readiness.

**Federal Trade Commission: Cybersecurity for Small Business** provides resources developed in partnership with CISA, NIST and the U.S. Small Business Administration to help small business owners understand and implement cybersecurity basics.

**Global Cyber Alliance: Cybersecurity Toolkit for Small Business:** Built for small to medium-sized businesses to address the Center for Internet Security Controls for preventing and/or reducing the most common attacks in today’s cyber threat landscape.

**National Cyber Security Alliance: CyberSecure My Business™** is a national program helping small and medium-sized businesses (SMBs) learn to be safer and more secure online, with a variety of resources and tools aimed at this stakeholder group.
ESSENTIAL ELEMENT: YOURSELF, THE LEADER

Build a network of trusted relationships for access to timely cyber threat information.
Maintain situational awareness of cybersecurity threats and explore available communities of interest. These may include sector-specific Information Sharing and Analysis Centers, government agencies, law enforcement, associations, vendors, etc.

Resources for Taking Action

CISA: CISA is responsible for protecting the nation’s critical infrastructure from physical and cyber threats. CISA.gov has a variety of cyber resources, training opportunities and information available at no cost to stakeholders.

National Council of Information Sharing and Analysis Centers (ISACs): Information Sharing and Analysis Centers help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards.

Multi-State Information Sharing and Analysis Center (MS-ISAC): The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation’s state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.

Information Sharing and Analysis Organizations (ISAOs): The ISAOs mission is to improve the nation’s cybersecurity posture by identifying standards and guidelines for robust and effective information sharing and analysis related to cybersecurity risks, incidents, and best practices. Similar to ISACs, but cross-sector in design.

Global Cyber Alliance: The Global Cyber Alliance is an international, cross-sector effort dedicated to eradicating cyber risk and improving our connected world. It aims to achieve this mission by uniting global communities, developing concrete solutions, and measuring the effect.

National Cyber Security Alliance: CyberSecure My Business™ is a national program helping small and medium-sized businesses (SMBs) learn to be safer and more secure online, with a variety of resources and tools aimed at this stakeholder group.

America’s Small Business Development Centers: Small business owners and aspiring entrepreneurs can go to their local SBDCs for free face-to-face business consulting and at-cost training. This website includes a number of cybersecurity resources for small businesses.
Lead development of cybersecurity policies. Business leaders and technical staff should collaborate on policy development and ensure policies are well understood by the organization. Perform a review of all current cybersecurity and risk policies to identify gaps or weaknesses by comparing them against recognized cyber risk management frameworks. Develop a policy roadmap, prioritizing policy creation and updates based on the risk to the organization as determined by business leaders and technical staff.

Resources for Taking Action

**NIST Cyber Security Resource Center:** The Computer Security Resource Center (CSRC) provides access to NIST’s cybersecurity and information security-related projects, publications, news and events. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

**SANS Information Security Policy Templates:** A library of comprehensive cybersecurity policy templates that business owners can use to inspire and optimize their own cyber policies. These templates cover a wide range of policy areas, including Network Security, Server Security, Application Security and more.

**Guide for Developing Security Plans for Federal Information Systems:** This guide for developing security plans for Federal information systems has a variety of useful technical data and guidance which can be used by a variety of non-Federal stakeholders as well.

**Cyber Readiness Institute: The Cyber Readiness Program** is a practical, step-by-step guide to help small and medium-sized enterprises become cyber ready. Completing the Program will make your organization safer, more secure, and stronger in the face of cyber threats. The Program also provides customizable policy templates focused on human behavior that address phishing, patching, passwords/authentication, and USB use.
Leverage basic cybersecurity training. Your staff needs a basic understanding of the threats they encounter online in order to effectively protect your organization. Regular training helps employees understand their role in cybersecurity, regardless of technical expertise, and the actions they take help keep your organization and customers secure. Training should focus on threats employees encounter, like phishing emails, suspicious events to watch for, and simple best practices individual employees can adopt to reduce risk. Each aware employee strengthens your network against attack, and is another “sensor” to identify an attack.

Resources for Taking Action

**National Initiative for Cybersecurity Careers and Studies (NICCS):** the NICCS Training Catalog provides a listing of cybersecurity and cybersecurity-related training courses offered in the United States.

**SANS:** Live and virtual computer security training developed by industry leaders and taught by real-world practitioners.

**FedVTS:** The Federal Virtual Training Environment (FedVTE) provides free online cybersecurity training to federal, state, local, tribal, and territorial government employees, federal contractors, and U.S. military veterans.

**Federal Trade Commission resources/Cyber basics:** training material on cybersecurity basics and best practices for businesses.

**Cyber Readiness Institute Cyber Readiness Program:** a comprehensive, self-guided tool containing information to reduce cyber risk, training material for employees, and more.
**ESSENTIAL ELEMENT: YOUR STAFF, THE USERS**

**Develop a culture of awareness to encourage employees to make good choices online.** Go beyond knowledge; identify the behavior you want to change and develop a cybersecurity strategy that targets cyber expectations. Define what success looks like through guidelines and policies. Continually reinforce cyber hygiene as you would other workplace hygiene (e.g. hand washing, professionalism, etc.). Create incentive structures that promote the formation of good habits (e.g. recognition for good behavior, loss of privileges for persistent reckless behavior). Encourage employees to participate in awareness campaigns like Stop. Think. Connect. and National Cybersecurity Awareness Month.

---

**Resources for Taking Action**

- **National Cybersecurity Awareness Month (NCSAM) toolkit**: comprehensive guide for individuals and organizations, regardless of size or industry, on engaging in and promoting cybersecurity awareness and developing effective practices that foster strong cybersecurity.

- **National Institute of Standards and Technology (NIST)**: introductory information for small business owners and leaders about cybersecurity, cybersecurity-related risks, and the importance of taking appropriate steps to secure your business.

- **National Cyber Security Alliance (NCSA): CyberSecure My Business**: a national program helping small and medium-sized businesses (SMBs) learn to be more secure online.

- **Global Cyber Alliance**: a free toolkit to help small to medium-sized businesses implement basic cyber hygiene which will enable business owners to significantly reduce the cyber risks they face every day.

- **FTC’s Talking cybersecurity with your employees**: learn the basics for protecting your business from cyber-attacks, developed in partnership with the NIST and Technology, the U.S. Small Business Administration, and the Department of Homeland Security.

- **Cyber Readiness Institute Cyber Readiness Program**: a comprehensive, self-guided tool containing information to reduce cyber risk, training material for employees, and more.
Learn about risks like phishing and business email compromise. Employees should be able to identify the trademark signs of malicious emails. Alert your staff to phishing and scamming tactics and include the latest changes in regular training. Regular updates and reminders keep everyone aware of current threats and how to handle them if encountered. Ensure employees know how and to whom to report suspicious emails or possible phishing attempts.

Resources for Taking Action

Federal Bureau of Investigation resources: solutions that businesses have employed to safeguard against e-mail compromise scams and criminal groups that engage in the scams.

FBI Internet Crime Complaint Center: the Internet Crime Complaint Center (IC3) accepts online Internet crime complaints from victims or from a third party to the complainant.

CISA Insights: this CISA Insight provides information on cyber phishing email attacks that non-federal partners can implement.

Global Cyber Alliance: DMARC setup guide, free, practical, real-world solutions that improve cybersecurity.

CISA Security Tips: Avoiding Social Engineering and Phishing Attacks: security tips for avoiding social engineering and phishing attacks and advice about common security issues for non-technical computer users.

Cyber Readiness Institute Cyber Readiness Program: a free compilation of information about what you can do to reduce cyber risk, along with training materials for your employees, and much more.
Identify and use available training resources. Organizations should know whether they already have training resources that are just being underutilized, or whether they should look outside of the organization to find these. Training your staff and promoting cyber awareness does not mean you have to create training materials from scratch. Many professional organizations, industry associations and academic institutions, as well as private sector and government networks provide ready-to-use cybersecurity training resources at no cost. Encourage your organization’s HR department to identify which resources are available to your industry.

Resources for Taking Action

ISACA: an international professional association focused on information technology governance and provides in-person training on tools and techniques from expert instructors.

National Initiative for Cybersecurity Education (NICE) framework Workforce Management Guidebook: key concepts to know and actions to take across your organization.

National Centers of Academic Excellence: designed to reduce vulnerability in our national information infrastructure by promoting higher education and expertise in cyber defense.

Small Business Administration (SBA): a national program that includes webinars, resources, and access to cybersecurity experts for small and medium-sized businesses.

National Cyber Security Alliance: broad-reaching education and awareness efforts to empower users at home, work and school with the information they need to keep themselves, their organizations, their systems and their sensitive information safe and secure online.


ISC2 Cybersecurity and IT Security Certifications and Training: webinars, videos, and more offering career advice, resolution to cybersecurity issues, and collaboration with peers.

Global Cyber Alliance: free, practical, real-world solutions that improve cybersecurity.
South Carolina
Critical Infrastructure
Cybersecurity Program (SC CIC)

S/A Sean Fay
Cyber Liaison Officer
South Carolina Critical Infrastructure Cybersecurity Program
sfay@sled.sc.gov
Priority Area #1 – Security information and event management (SIEM)

Priority Area #2 – Security Training

Priority Area #3 – Endpoint (and end user) security

Priority Area #4 – IT Staffing and Technical Training

Priority Area #5 – Critical Technology Infrastructure Improvements

Priority Area #6 – Security Services

Priority Area #7 – Telework Improvements
CORONAVIRUS
2019-nCOV
COUNTIES PROVIDE LOCAL SERVICES CRITICAL TO AMERICA’S COVID-19 RESPONSE AND RECOVERY

Learn more about the county role in addressing the COVID-19 pandemic:
https://www.naco.org/resources/counties-matter-covid-19
I changed all my passwords to "incorrect".

So whenever I forget, it will tell me "Your password is incorrect."