SVAM INTERNATIONAL, INC.

Putting Information Technology To Work™

www.svam.com

New York State Cyber Security Conference

BUILDING STRONGER CYBERSECURITY COMMUNITIES

DRIVING AWARENESS AND TRAINING FOR A MORE SECURE DIGITAL WORLD

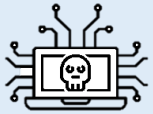
Speakers:
Kiran Bhujle
Shahryar Shaghaghi

June 7, 2023

Agenda

Why Cybersecurity Matters

Current Threat Landscape and Emerging Threats



Cyber Crime

Risk Culture

The Power of Community

Awareness & Training Strategies

Call to Action

Speakers

Kiran Bhujle

SVAM Cybersecurity Practice Leader
kbhujle@svam.com

Global Managing Director at SVAM International, Kiran oversees SVAM's Security Advisory Group, with over 25 years of experience in IT Risk and Cybersecurity.

- Previously Cyber & Technology Risk Client Executive at CohnReznick, Access Risk Transformation Leader at Ernst & Young, IBM Global Business Services, and Deloitte.
- Harvard Business Review - Cybersecurity Advisory Board.
- Forbes Technology Council - Executive member.
- Adjunct faculty at Columbia University focusing on IT Risk Management and Operational Risk Management courses for the Enterprise Risk Management Masters Program.

Shahryar Shaghaghi

Technology, Risk Management, and Cybersecurity Executive
sshaghaghi@svam.com

Senior technology and risk management executive focused on cybersecurity and data privacy programs, with over 30 years of experience in various organizations and leadership roles.

- Professor of Practice at Columbia University for five years, focusing on IT Risk Management and Strategic Communications courses for the Enterprise Risk Management Graduate Program.
- Ex-partner with Deloitte, BDO, Kurt Salmon, CohnReznick, and Executive VP IT Risk at Citibank.
- As a member of AICPA's Center for Audit Quality (CAQ) and Assurance Services Executive Committee (ASEC) Shahryar co-developed SOC for Cybersecurity (SOC 3) attestation framework.

Introduction

Cybersecurity refers to the practices, technologies, and measures designed to protect computer systems, networks, and data from unauthorized access, damage, or theft. It involves various components such as network, information, and application security.

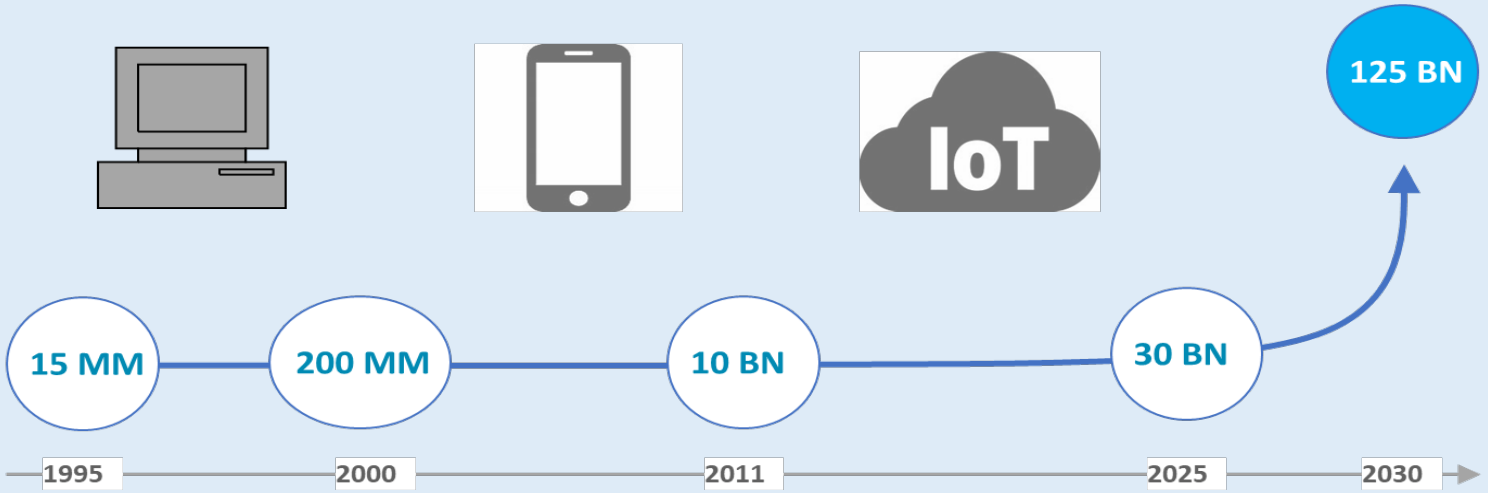
- Cybersecurity is a critical concern for both individuals and organizations.
- Today, we will discuss the importance of community-building in driving cybersecurity efforts.
- We will explore the benefits of creating a security culture and leveraging a community's collective knowledge and skills.
- Additionally, we will examine effective strategies for increasing cybersecurity awareness and providing training.

Why cybersecurity matters

[1] ISC2 Cybersecurity Workforce Study 2022 [2] Statista 2023 [3] IBM Cybersecurity Survey

Threat landscape

- Digital transformation will continue, and therefore cybersecurity landscape is constantly evolving.
- There are more devices attached to the internet today than the world population. Due to IoT, by 2025, we will have more than 30 billion internet-attached devices.
- Artificial Intelligence (AI) and upcoming quantum technology increase the complexity of cyber defense.
- Since hackers only need to be right once, and those who protect the organization must always be right, your cybersecurity program must constantly evolve.
- To evolve, it is vital to understand who is after you, what motivates them, and what they are after.



Source: Cisco

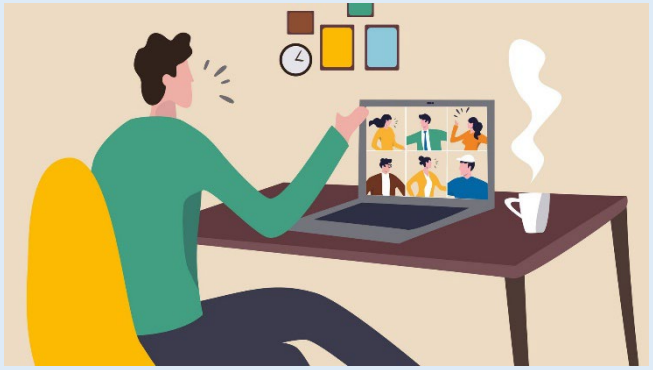
Top cyber threats

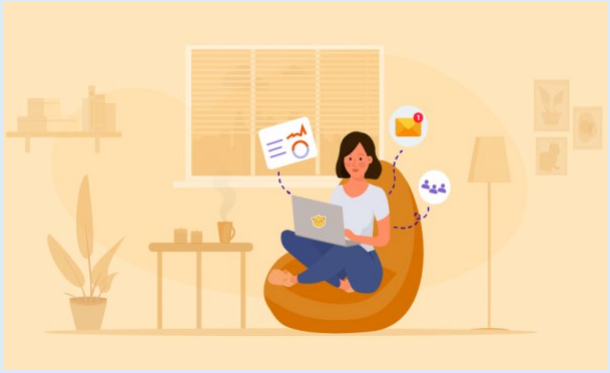
- Pandemic-driven digital transformation (remote work) has empowered cybercriminals to enhance their capabilities and swiftly target vulnerable victim groups with greater precision.

- Organizations unprepared for the remote landscape face a disadvantage in preventing and responding to security incidents, potentially exposing themselves to data breaches.

Remote work security

- Poorly secured home networks can bring viruses and malware into company networks through computers that have been connected to them.
- Routers should have a strong, unique password containing at least 16 characters and capital letters, numbers, and symbols. Do not use the default password that came with the device.
- Create a guest network to be used by friends, family, and visitors.
- Do not leave laptops or tablets out if you have visitors you don’t know well.
- Be mindful of where you are printing sensitive information.





Social engineering

Social engineering manipulates people into performing actions or divulging confidential information. Similar to a confidence trick or simple fraud, the term applies to deception to gain information, commit fraud, or access computer systems.

Phone Call: This is John, the System Admin. What is your password?

Email: ABC Bank has noticed a problem with your account…

In Person: What ethnicity are you? Your mother's maiden name?

I have come to repair your machine…

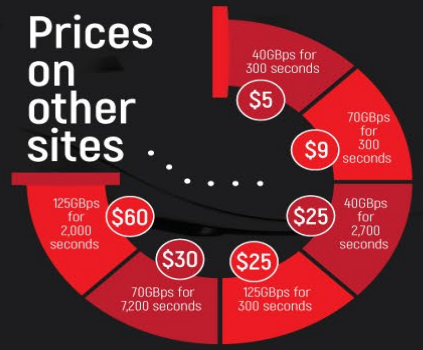
and have some software patches

Price list for Cyber Crime

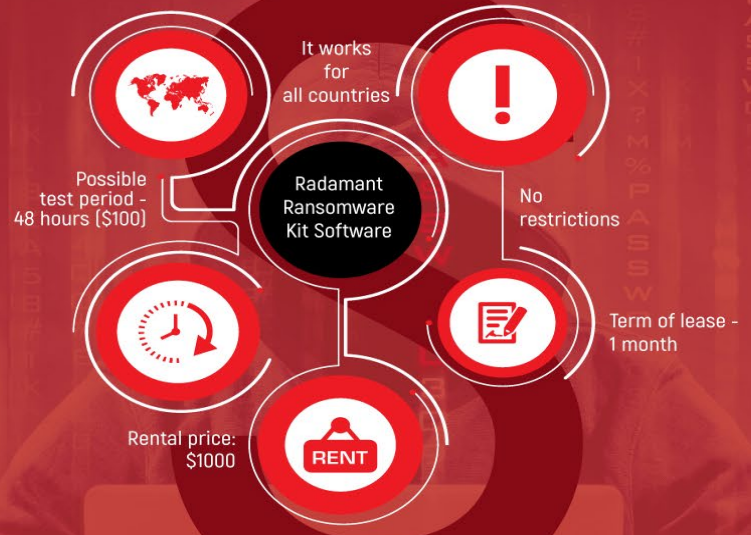
SVAM INTERNATIONAL, INC.

DDoS ATTACK

*Here, an hourly price wasn't specified, so a price of $2.50 ($60/24 hours = $2.50) was used.



RANSOMWARE



Radamant Ransomware Kit Software encrypts data and demands users to pay .5 Bitcoins to get files back. The Ransomware was advertised on dark web with features listed above.

Malware Karmen, "ransomware as a service" (RaaS) derived from "Hidden Tear," an open source ransomware project, available for purchase by anyone was priced at $175.

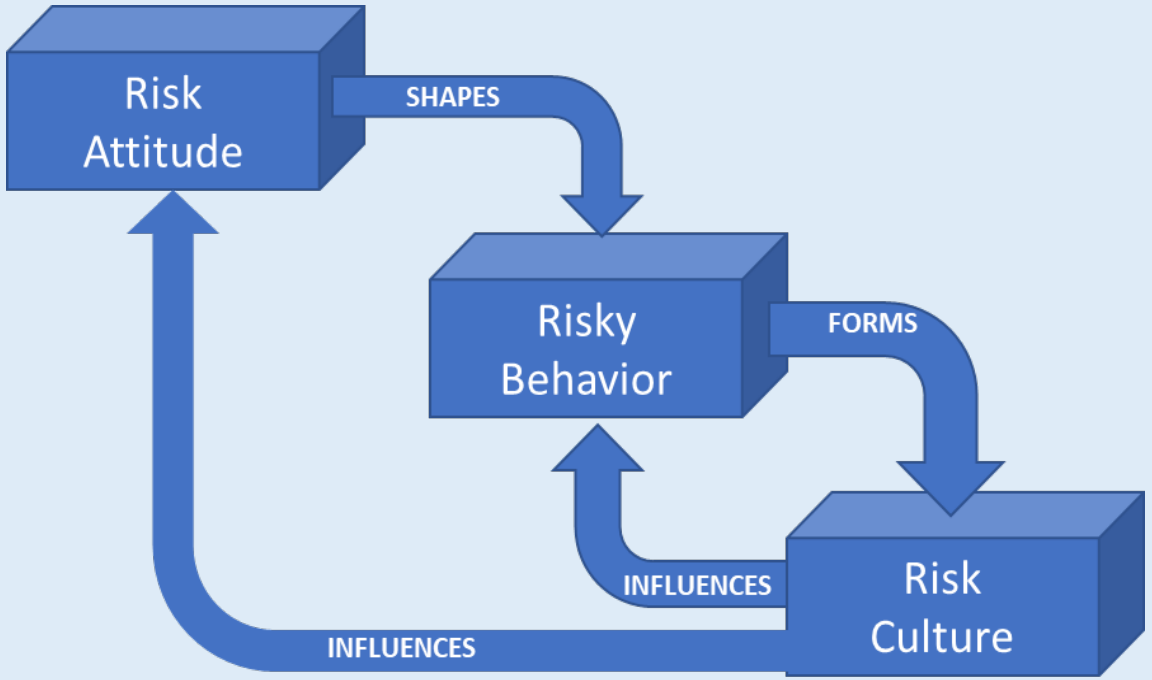
USER CREDENTIALS

Stolen identity and financial information are available in all shapes and sizes, with prices going"

SOURCES:
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-north-american-underground.pdf
https://www.mcafee.com/us/resources/reports/rp-hidden-data-economy.pdf
https://www.bleepingcomputer.com/news/security/radamant-ransomware-kit-for-sale-on-exploit-and-malware-sites/
https://www.arbornetworks.com/blog/asert/estimating-the-revenue-of-a-russian-ddos-booter/
https://www.scmagazineuk.com/ransomware-as-a-service-being-sold-for-175-on-dark-web/article/651138/

Risk culture

- A strong risk culture is essential for an organization to operate safely, soundly, and ethically.
- A robust culture cultivates desired behavior, leading to optimal organizational performance.
- Risk culture and work culture are interconnected, as an unhealthy work culture poses undeniable risks to the organization.
- Promoting the value of doing the right thing based on personal conviction.
- Diversity and inclusion are critical for cultivating the right culture as they facilitate collaboration and enhance decision-making.
- Observable behavior is the primary driver that shapes culture.
- Other specific drivers form the foundation of every successful culture: trust, ethics and integrity, quality, customer focus, and spirit and vitality.

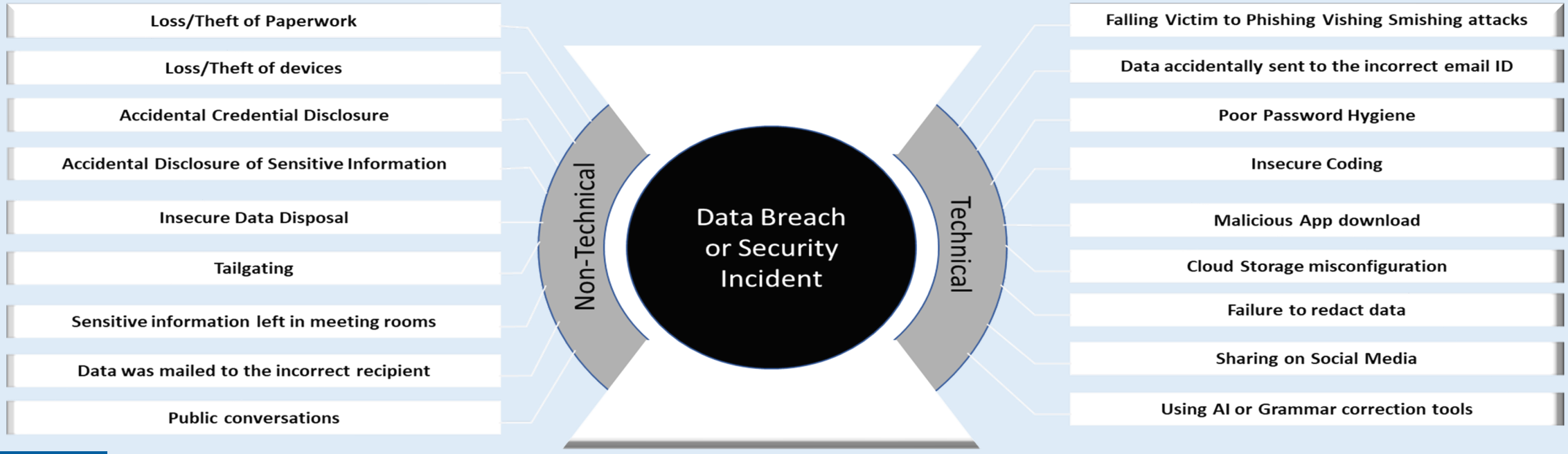


Importance of a security culture

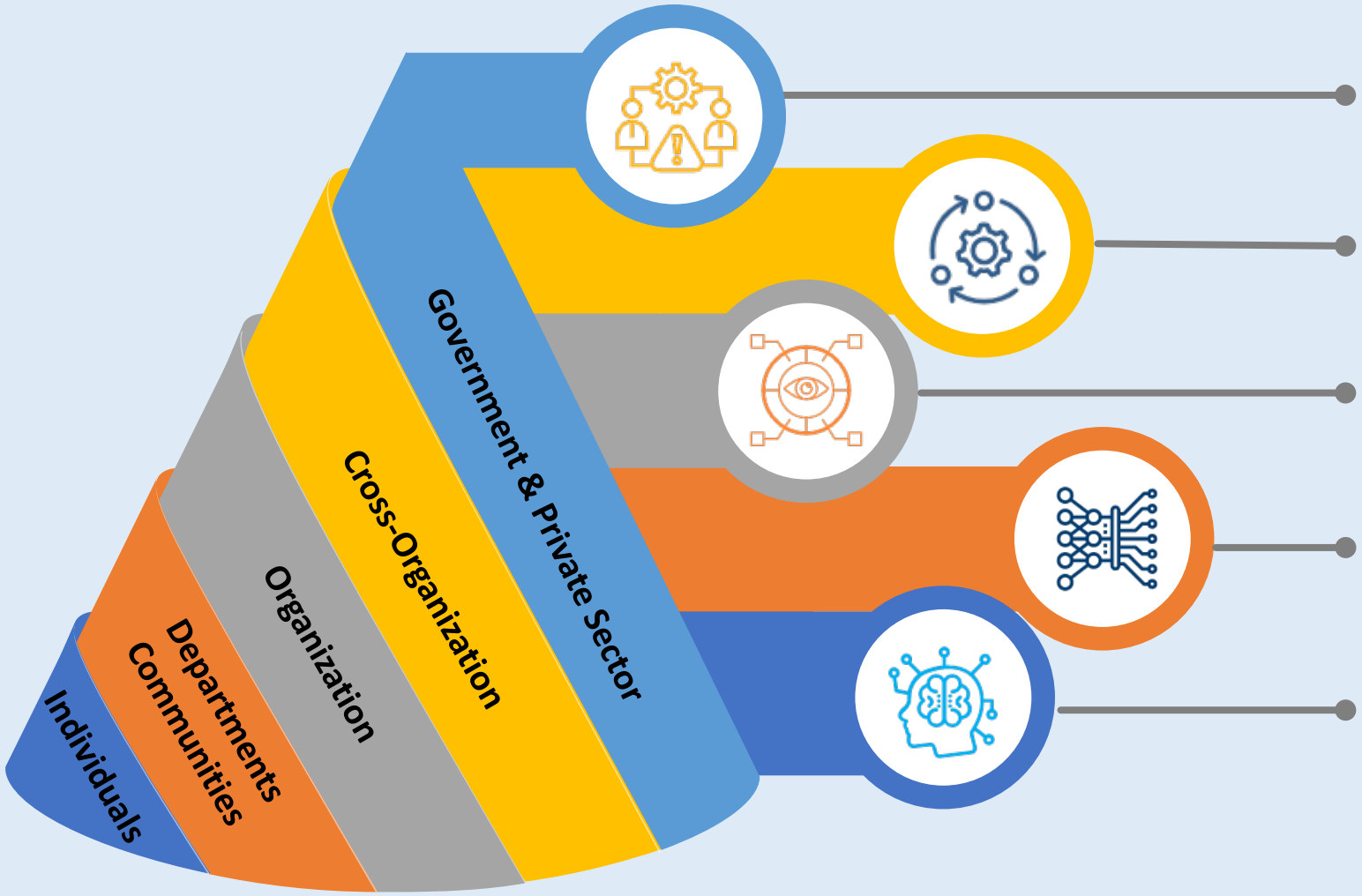
- In a strong security culture, employees take ownership of cybersecurity. They report suspicious emails, follow protocols, and actively participate in training. Open communication fosters a proactive approach to protecting sensitive information.
- In a security-conscious school, students and teachers adhere to cybersecurity guidelines. They prioritize strong passwords, device security, and cautious online behavior. The curriculum integrates security awareness and equips students to recognize and respond to cyber threats, fostering a safer digital environment.
- In an online community, trust and accountability bolster security. Users report suspicious activities, and moderators diligently monitor the platform. A culture of trust enhances vigilance and fosters a safe and secure environment for all members.

Securing cyberspace starts with YOU

- Hackers are actively targeting individuals, their personal data, and their access to corporate information.
- Gaining access to your login information enables hackers to impersonate you and infiltrate your organization's systems and data.
- The potential consequences extend to compromising the security of your client's information.
- While technology plays a vital role in security, it can only address a FRACTION of the overall risk landscape.
- Combining technology with proactive measures and HUMAN awareness is essential to strengthening the security posture of individuals and organizations.



The power of community



Government & Private Sector

Engage in information sharing and collaboration to combat cyber threats.

Cross-Organization (ISAC)

Establish partnerships with organizations and institutions for broader impact.

Organization

Advocate for cybersecurity awareness and policies at local and global levels.

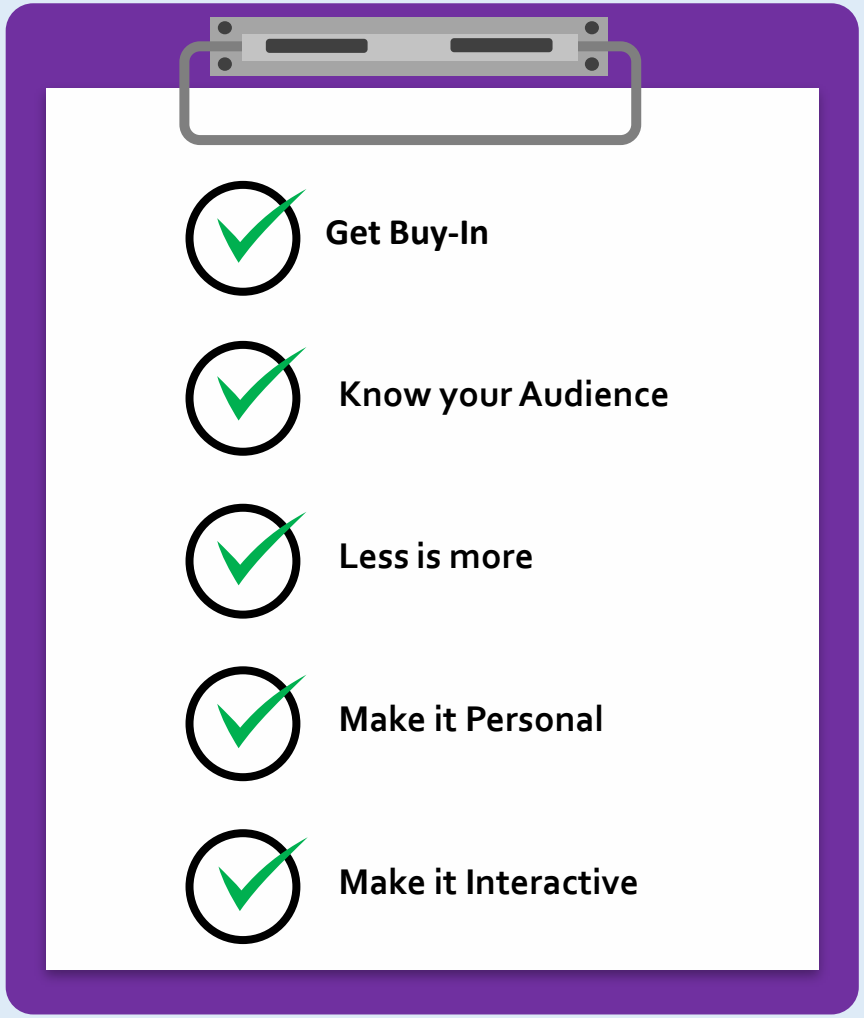
Departments/Communities

Share resources, best practices, and knowledge within the community.

Individuals

Stay informed, be vigilant, educate others, and report suspicious activities.

Security awareness training - Keep it simple



Know your audience

- Relate topics to their everyday experiences.
- Speak their language, and avoid technical jargon.
- Avoid discussing back-office tools they can't control.
- Utilize visual aids.

Less is more

- Keep slide count concise.
- Avoid excessive statistics.
- Foster interactivity instead of lecturing.
- Focus on core concepts, and avoid overload.
- Keep it current.

Make it personal and interactive

- Tell relatable stories within their industry, regional area, company, or department.
- Emphasize the need for buy-in from senior management.
- Move beyond training videos and engage in interactive approaches.
- Discuss security tips on a personal level.

Amplify the effectiveness

- Conduct regular phishing simulations.
- Send newsletters with up-to-date and relevant information.
- Display informational banners around the office.
- Incorporate games with prizes.
- Organize lunch and learn sessions.

Alert authorities of suspicious behavior

- Upon suspicious behavior or actions, notify the appropriate individuals and/or IT.
- Do not assume the breach is too small to warrant IT's attention.
- Protecting confidential information is a business, ethical, and legal requirement.
- Examples of suspicious behaviors or actions:
  - Strange activity on your computer/laptop (e.g., pop-ups, very slow)
  - Strangers ask questions about security, building security procedures, or other sensitive information
  - Briefcase, suitcase, backpack, or package left behind
  - Intruders in secure areas where they are not supposed to be

Compromised, Now What?

- Disconnect from the internet
- Change passwords
- Activate 2FA on your accounts wherever possible
- Monitor accounts and statements
- Scan for malware
- Inform relevant parties
- Learn from the incident

Seek assistance from cybersecurity professionals or experts if needed to ensure a thorough investigation and remediation of the hack.

Call for Action

By working together, sharing knowledge, and investing in continuous education, we can create a more secure digital environment for all.

- All American citizens/residents must do their part—in their work and personal life—to ensure that cyberspace is a safe and secure environment for all Internet users
- By following simple steps to protect yourself online, you can deter threats caused by identity thieves, fraud and phishing scams, cyber bullies, and cyber predators
- Raise awareness about online safety by being a source of information for your family, friends, and co-workers
- Stop.Think.Connect. is a "peer-to-peer" campaign designed for Americans just like you

- **Resources**

  FBI Cyber Security webpage
  - https://www.fbi.gov/about-us/investigate/cyber

  DoD Social Media Hub
  - http://dodcio.defense.gov/Social-Media/

  Stop Think Connect
  - https://www.stopthinkconnect.org/

  Cybersecurity & Infrastructure Security Agency (CISA)
  - https://www.cisa.gov/resources-tools/resources/stopthinkconnect-toolkit

Q&A

SVAM INTERNATIONAL, INC.

Thank you!

Contact information

Kiran Bhujle

kbhujle@svam.com

908-590-1445

Shahryar Shaghaghi

sshaghaghi@svam.com

917-972-9313