How To Effectively Keep Your Organization Cyber-Secure In An Ever-Changing Digital World

SHIRA RUBINOFF

PRESIDENT, PRIME TECH PARTNERS

@SHIRASTWEET

SHIRA@SHIRARUBINOFF.COM

We Will Discuss:

1) How an Organization Can Achieve Proper Cyber Hygiene

2) How To Deal With - Insider Threats

   4 Types

3) How To Achieve Proper Cyber Hygiene Protocols From Employees

Compliance Culture vs Security Culture

Compliance Culture

- Policies come from top down
- Policies enforced by threats of punishment
- Security team attitude defaults to PEBKAC (problem exists between keyboard and chair)
- Non-security staff sees security as someone else’s problem

Security Culture

- Polices are formed with input from ALL stakeholders
- Policies enforced consistently & good security behavior rewarded
- Security Team studies workflows and brainstorms solutions
- Security is everyone's responsibility

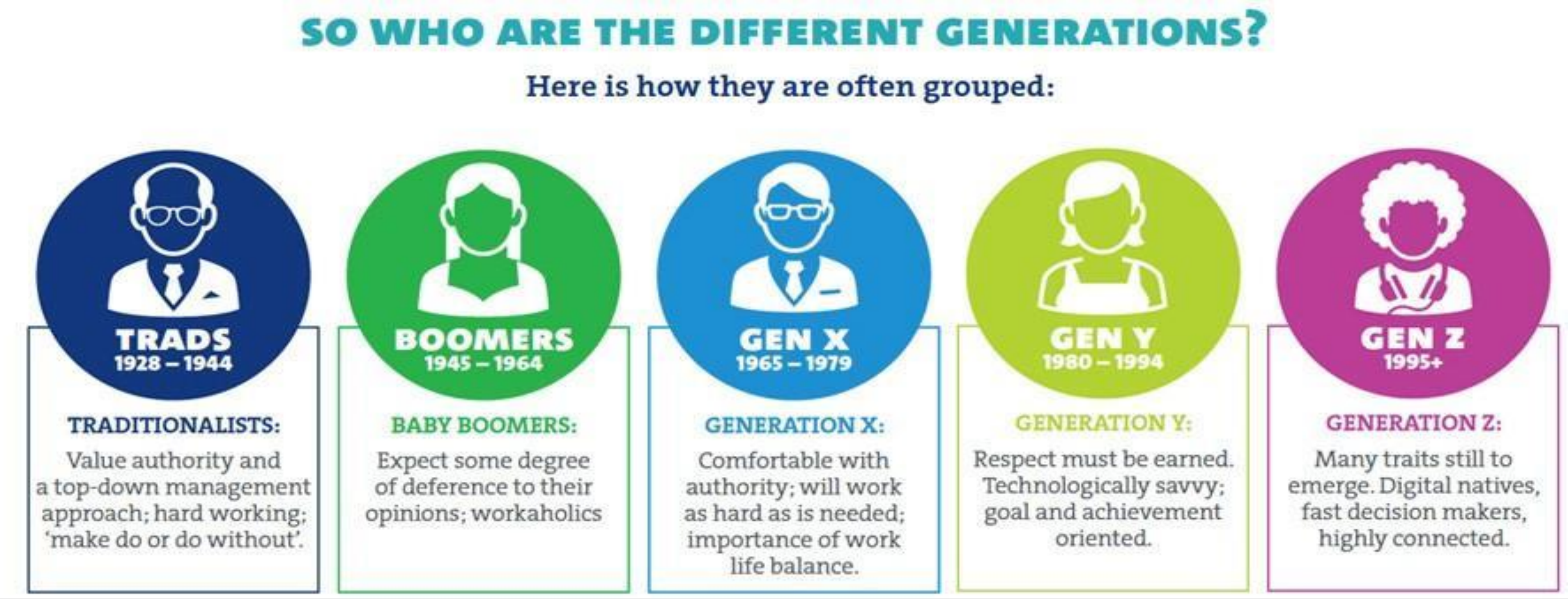
Cyber Hygiene in an Organization

Proper CYBER HYGIENE has many elements that need to be addressed including:

- 1) Continuous Training for ALL employees no matter what level or job they have within the organization.
- 2) Global awareness throughout the organization.
- 3) Updated security implemented on a regular basis
- 4) Implementing a Zero-Trust model

Continuous Training & Awareness for ALL Employees

- **From Consultant to Intern to CEO**
- **Generational** appropriate training – make it meaningful



SO WHO ARE THE DIFFERENT GENERATIONS?

Here is how they are often grouped:

TRADS
1928 – 1944

TRADITIONALISTS:
Value authority and a top-down management approach; hard working; 'make do or do without'.

BOOMERS
1945 – 1964

BABY BOOMERS:
Expect some degree of deference to their opinions; workaholics

GEN X
1965 – 1979

GENERATION X:
Comfortable with authority; will work as hard as is needed; importance of work life balance.

GEN Y
1980 – 1994

GENERATION Y:
Respect must be earned. Technologically savvy; goal and achievement oriented.

GEN Z
1995+

GENERATION Z:
Many traits still to emerge. Digital natives, fast decision makers, highly connected.

Training should include…

- Stage real-world specific scenarios

- Discussions over past problematic instances and how to rectify them going forward

- Assurance of management support = TEAM EFFORT

- Leave time for dialogue – feedback and Q& A

Remember: New vs Old of Training

NEW	OLD
frequent	annual
incremental	info dumps
situationally relevant	universally applicable

Updates; Security Implemented on a Regular Basis

Implement A Zero-Trust Model

Building a Culture of Security

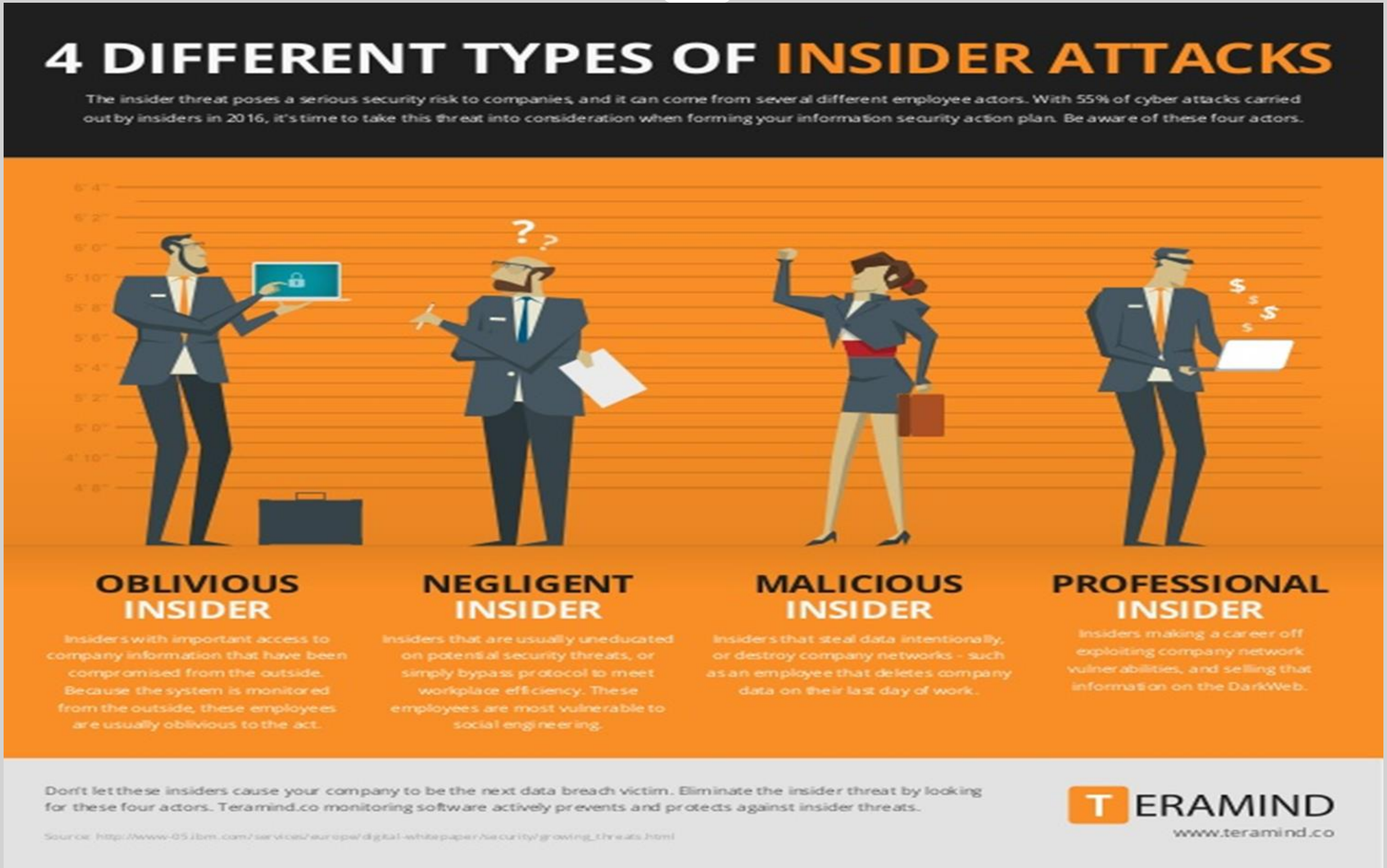
Keeping Your Security Streamlined Across Your Organization is Critical

- Employee freedoms are unrestricted when possible
- Security-based restrictions are explained when they occur
- Understanding protocol in the organization imperative - and consequences and accolades are consistent
- Management values security and its employees

Insider Threats

- Insiders are the most studied risk to security in academic literature
- Insider threats predate computing
- Connectivity and data portability increase risks posed by insiders
- Insiders are a component in 50-75% of all data breaches

Four Types of Insider Attacks



4 DIFFERENT TYPES OF INSIDER ATTACKS

The insider threat poses a serious security risk to companies, and it can come from several different employee actors. With 55% of cyber attacks carried out by insiders in 2016, it's time to take this threat into consideration when forming your information security action plan. Be aware of these four actors.

OBLIVIOUS INSIDER

Insiders with important access to company information that have been compromised from the outside. Because the system is monitored from the outside, these employees are usually oblivious to the act.

NEGLIGENT INSIDER

Insiders that are usually uneducated on potential security threats, or simply bypass protocol to meet workplace efficiency. These employees are most vulnerable to social engineering.

MALICIOUS INSIDER

Insiders that steal data intentionally, or destroy company networks - such as an employee that deletes company data on their last day of work.

PROFESSIONAL INSIDER

Insiders making a career off exploiting company network vulnerabilities, and selling that information on the DarkWeb.

Don't let these insiders cause your company to be the next data breach victim. Eliminate the insider threat by looking for these four actors. Teramind.co monitoring software actively prevents and protects against insider threats.

Source: http://www-05.ibm.com/services/europe/digital-whitepaper/security/growing_threats.html

TERAMIND
www.teramind.co

Two types of malicious insiders (Shaw 2005) (malicious and professional)

Opportunistic Employees

- Motivated by greed
- Any gender
- Access (physical or digital)
- Skills (technically proficient)
- Moral neutralization
  (ability to rationalize the illicit act)
- Recent (past six months) adverse event at
  work or in personal life

Disgruntled Employees

- More likely to be male
- Sense of entitlement
- A history of negative social and personal behaviors
- Lack of social skills or strong social isolation
- Recent inciting incident

Combating malicious insiders

Combat Opportunistic Employees with…

- Position rotation and cross-training
- Mandatory vacation policies
- Regular Audits
- Visible Monitoring
- Transparent and rapid sanctions

Combat Disgruntled Employees with…

- Access controls
- Clear role boundaries
- Cross-functional Teams
- Management training to recognize problematic behavioral changes
- Robust and automatic post-termination protocols

Non-malicious Insiders (oblivious and negligent)

They don’t mean any harm…

- Uninformed
- Indecisive
- Unsuspicious
- Unsure of support
- This vulnerability can be minimized with good, ongoing training

To Achieve: The Situationally Compliant Employee:

- Build Trust

- Support their values

- Align security with work, rather than work with security

- 360 feedback

- Invest in a security culture

Which will Result In:

- Successful in their roles
- Aware of information security policies
- Technically competent
- Sensitive to the security culture of your organization
- Motivated by their own job-related values

Thereby Yielding Proper Cyber Hygiene Protocols From Employees

Thank you for listening to my presentation!

Please follow me :

Twitter: @ShirasTweet

LinkedIn: www.linkedin.com/in/shirarubinoff