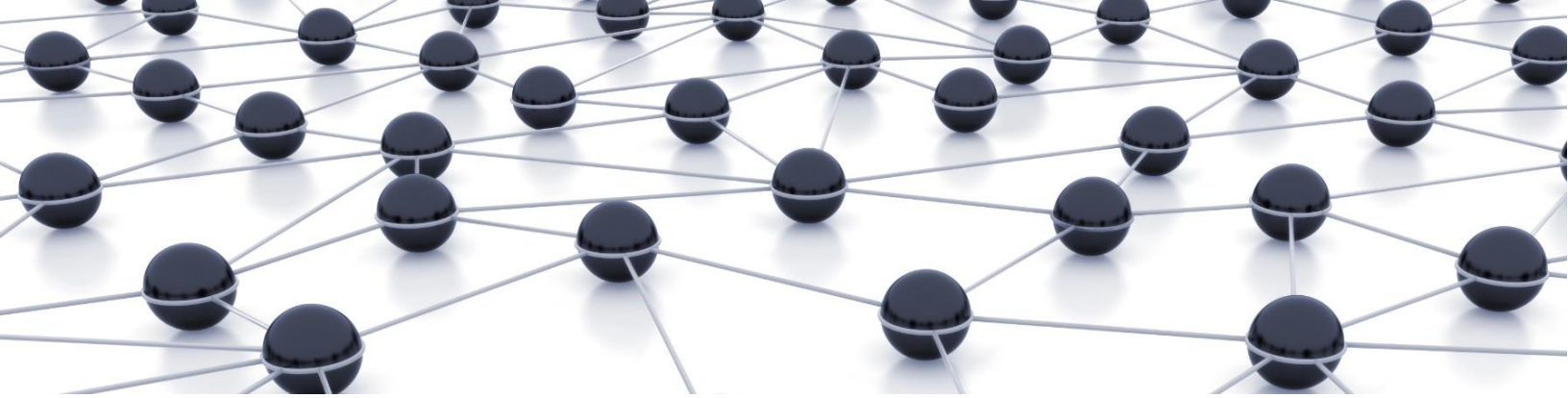

IntelliSyn

Desktop-to-Cloud Business Communications

# Organizational Behavior Transformation to Defend Against Social Engineering of Access to IT Systems

By Merv Perry MBA MSc CISSP CISM

A new generation of employees is transforming the workplace where being socially connected and accessible at all times poses a challenge to defend IT system and sensitive business operations from social engineering attacks. It is a generation that has grown up with social media tools that challenge the concepts of what is privacy and what is confidential. Access to social media tools in the workplace like Facebook, Twitter, and Instagram means that the risk of information leakage is far greater with the next generation of workers than just 15 years ago. The shared economy means there is more information on every individual employee, and it is available for use to orchestrate a social engineering attack to access corporate IT systems and affect sensitive business operation.

*The application of role playing and scenario analysis of information security policies are organizational behavioral strategies to combat social engineering attacks.*

An employee may easily be duped into action, or they lack proper critical analytical skills to understand the necessary due diligence needed to access what is confidential. They may react to what they see, hear, or read on the Internet as being normal behavior rather than the exception to pass out information when confronted with an attack. The application of role playing and scenario analysis of information security policies are organizational behavioral strategies to combat social engineering attacks. Reinforcing countermeasures requires periodic attacks to test an organization's vulnerability, and attacks are confidentially arranged with senior management and professional social engineering penetration testers. These testers adjust their methods of access with current social trends to determine how far into the organization they can penetrate to gain access or disrupt sensitive business operations before they are possibly detected.

Being socially connected and accessible at all times poses a challenge to defend IT systems and sensitive business operations from social engineering attacks when the employees seem less concerned with its importance. In some cases, it appears to be generational, with a higher risk for those who are referred to a Millennials. Just why this is happening requires some reflection on the history of the past four decades as each generation has grown up through increased suspicion of authority and government secrecy and corporate misdeeds. Boomers grew to dislike authority and social restrictions from their parents, which influenced how Boomers were to raise their children, and those children became the parents (Generation-X) of today's Millennials (born late 90's and early 2000s).

*Millennials had access to the Information Age's greatest wonder, the Internet.*

Millennials have grown up with rapid changes in technology, and at a pace that is a hundred times faster than the previous two generations knew. They saw their parents squeezed by recessions, stock market crashes, layoffs, and lost job opportunities with social upheavals in what and what not to trust from leaders in government and industry. Their parents sought to protect them and saw that they had access to the Information Age's greatest wonder, the Internet. It arrived without full knowledge of what it might become and had no restrictions. However, the advent of a web browser made it more readily available to those persons who could afford a connection. The capacity of broadband communications expanded with faster technologies (e.g., fiber optics and faster microprocessors with large memory sizes to store or execute programs) leading to evermore improvements. The arrival of email and file transfer protocols to download material or exchange files with others across a continent was the moment, in my opinion, where the sharing economy began to take off, as well as the rise of security threats that were not previously conceived.

*Millennials were provided digital devices without being taught how to use them.*

I'm not picking on this new generation of workers for a fault they made themselves, but for their reaction to how they adapt to what is the norm. They were taught to share their toys and express their feelings to others – even strangers in the group. Their schools and parents often provided digital devices to young people without teaching them how or why to protect the device and themselves.

Millennials feel work has to be an expression of themselves and they have to consider themselves significant to others around them at all times. The arrival of digital cameras in cellphones, Youtube,

Facebook, Twitter, and Instagram is their means of sharing themselves with others at all times. They may react to what they see, hear, or read on the Internet as being normal behavior rather than the exception. And they think it is normal to pass out what the previous generations considered confidential and private information. The opinion leaders of this generation are not the politicians of the past or heroes of some conflict, instead it is anyone who can master the social media to gain the greatest "likes" and connections. The gratification comes from not what was done, but more from those you connect with for validation of your actions. If you do not like your boss, company, or a social issue, then you express it with no reserve or concern of the long-term consequences. It is done in an instant and circulates forever. The shared economy means more information on every individual employee is available for use to orchestrate a social engineering attack to access corporate IT systems, and affect sensitive business operation.

Intellisyn Communications has a staff with a combined experience of 120 years in technology and business, which ranges in age from the late twenties to early seventies. This diversity is our strength in developing secure desktop-to-cloud solutions, and we bridge the multiple generations that many organizations face with the implementation of new technologies.

To quote a line from a song called "In the Living Years" from Mike + TheMechanics, an English Pop/Rock supergroup formed in 1985.

*"Every generation blames one before, all their frustrations come beating on your door"*

---

*The policies you write need to be very short, directed, and clear — along with including details where it is necessary to explain their importance.*

---

If you're the manager responsible for the transformation of your IT and organization, then you will relate to this quote if it is your door they beat upon. This is very true when it comes to security and social engineering and today's workforce. The policies you write need to be very short, directed, and clear — along with including details where it is necessary to explain their importance. Millennials will make pretty good decisions if given the information in bite-sized pieces. Do not you write clunky policies with no real-world examples to support your case. Be clear and concise to get adherence. It takes more effort to reach them.

The US Federal Bureau of Investigation (FBI) Citizen's Academy teaches issues related to cyber security and the Bureau's techniques for the investigation of community leaders. When the FBI sent a phishing scam to test its academy's participants via their email addresses, every participant except two fell for the scam. Many organizations are now testing their employees in much the same way the FBI tested its participants. You can phish your employees through an internal effort or by hiring outside security

consultants. Either way, the goal is to find out which employees are following policy and which ones need further training. Training is the first priority, but employees and others who are not following workplace policies must be held accountable. This is important for all employees, but perhaps more so for millennials. Millennials are known as the 'me' generation. They want immediate gratification, and sometimes they do not seem to care about the company or its reputation. When this situation happens, the organization is left with no choice but to take corrective actions, including dismissal.

*Reinforcing countermeasures requires periodic attacks to test an organization's vulnerability and attacks are confidentially arranged with senior management and professional social engineering penetration testers.*

The application of role playing and scenario analysis of information security policies are behavioral organizational strategies to combat social engineering attacks. Reinforcing countermeasures requires periodic attacks to test an organization's vulnerability and attacks are confidentially arranged with senior management and professional social engineering penetration testers. These testers adjust their methods of access with current social trends to determine how far into the organization they can penetrate to gain access or disrupt sensitive business operations before they are possibly detected.

I recommend reading an article by Joan GoodChild, Senior Editor of CSO, about social engineering expert Chris Hadnagy (February 9, 2011). He tells of successful cons he's seen as a security consultant, and six prevention tips

*A security culture must engage people with different areas of expertise (e.g., security, compliance, privacy) to work together toward clearly defined goals based on business priorities*

Ultimately, it boils down to corporate culture from the top down, and building a security culture which engages people with different areas of expertise (e.g., security, compliance, privacy) to work together toward clearly defined goals based on business priorities, as well as giving brief progress reports daily and adjusting priorities based on the developing situation.

The following strategies will help reduce the risk of failure and the impact of incident:

- Create a cross-functional team that is the first to respond to the incident and develop subsequent processes to mitigate the impact. Include members from information security, privacy, compliance, legal, and any other departments.
- When an incident occurs, the whole team must be notified. This gives each functional area time to determine what actions to take and if it is feasible.
- The team must meet regularly and review security events to ensure that potential incidents do not fall through the cracks. Team members will become more aware of the needs of other functional areas, share progress, discuss business priorities, and plan next steps.
- An integral part of the response process is to ensure that the proper tools and processes are in place for sharing and documenting information.

I recommend a book called "*Build A Security Culture*" by Kai Roer.

From the book's cover and website

> "Kai Roer presents his Security Culture Framework, and addresses the human and cultural factors in organizational security. The author uses clear, everyday examples and analogies to reveal social and cultural triggers that drive human behavior. He explains how to manage these threats by implementing an effective framework for an organizational culture and how to ensure that your organization is set up to repel malicious intrusions and threats based on common human vulnerabilities."
>
> "Human behavior is complex and inconsistent, making it a rich hunting ground for would-be hackers and a significant risk to the security of your organization. An effective way to address this risk is to create a culture of security. Using the psychology of group behavior and explaining how and why people follow social and cultural norms, the author highlights the underlying cause for many successful and easily preventable attacks."