Edward Liebig
08/04/2022

Security Culture: An OT Survival Story

Most members of the security community acknowledge the need for a renewed and improved "security culture" — meaning systemic corporate awareness, measurement, and monitoring for improvement of cybersecurity in order to help lower the overall risk landscape. Just look at Kim Zetter's Black Hat USA 2022 keynote, which called for crucial security improvements throughout critical infrastructure. Many times, the impediment to effective security is not necessarily technical, rather a cultural issue. However, many often mistakenly equate "user education and training" with "the creation of a security culture." User education is about information sharing on issues and obligations —whereas security culture is about behavioral changes in support of security. In other words, defining culture can be a daunting task, but Professor John McAlaney from Bournemouth University, UK did a nice job when he defined it as, *"Attitudes, assumptions, beliefs, values, and knowledge that employees/stakeholders use to interact with the organization's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behavior (i.e., incidents) evident in artifacts and creations that become part of the way things are done in the organization to protect its information assets. This information security culture changes over time."*

Building Security Culture Through User Awareness

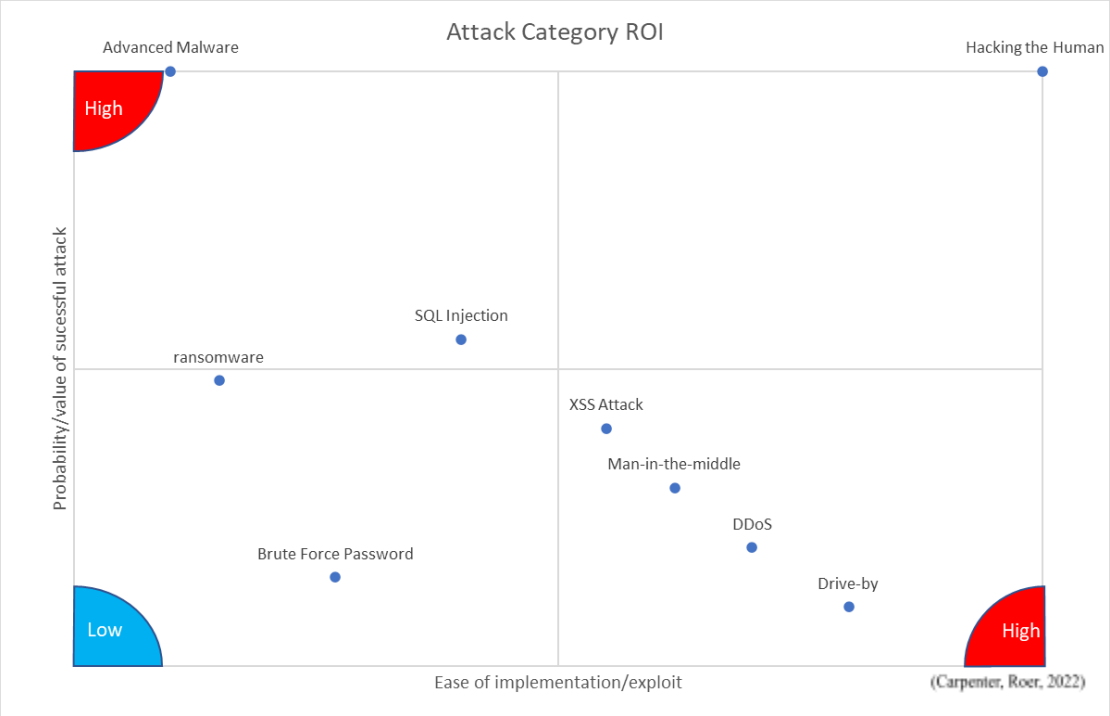
Though user awareness and building a security culture are two very different exercises with distinct challenges, they share one commonality*:* They require serious attention and support. Interestingly enough, with that in mind, these two exercises actually complement each. Consider this: While there are many debates on Chief Information Security Officer (the de facto owner of user awareness) reporting structures and how the role reports up to the CEO, the support necessary for driving a security culture is not dependent upon this hierarchy; it's dependent on the modification of user behavior through generally accepted business operations. This holistic business process modification is why the security culture needs to be driven from the top down. Most security professionals accept that user awareness is one of the best investments in a security organization's arsenal of security tools. User awareness should be baked into an

organization's security tools and take place as consistently as searching the systems for Indications of Compromise (IoC). User awareness does not take the place of, or is it the same as, the creation of a security culture — rather it is a necessary component of any effective security culture.

Getting on Board

Ownership and support for creating a security culture must be driven at the Board level. This is because while many exploitations and "attacks" are no more than another security alert to manage, when a skilled adversary gets involved, serious risks arise. As Edward Liebig once said, "Amateurs hack systems; professionals hack people."

"Hacking the human" as a security risk category has a very high yield of success and transcends technological safeguards.



The trick is to protect the human operator from "the pitfalls of human nature" by controlling and sculpting behavior. This behavior modification may often require critical thought about ingrained business practices. Support for the realization of necessary changes will rely heavily upon top-down influence.

Security Culture in OT Environments

Operational Technology (OT) environments are saddled with an even more significant challenge in examining and cultivating their overall security culture. Not only do the business users play an integral role, but the OT engineers are just as vital to preventing and responding to cyber and security events. The dichotomous yet symbiotic relationship between IT and OT is where the creation of a holistic security culture will need top-down support to look critically at the overall business and operational processes. Things that can torpedo the most earnest attempts at shoring up a security effort could be as unsuspecting as the accounting process for applying budgets across the individual locations/plants. Or the "perception of ownership" for security. "Are security challenges an IT issue to drive?" If so, are cultural impediments to successfully addressing Incident Response (IR) and recovery from security events across both IT and OT? Or is IR a collaborative process between IT and OT system owners? Most C -level executives would believe the latter to be true. In that case, is there an overall governance function across IT/OT and business functions like Legal, Accounting, Corporate Communications, etc. that drives efficiency and QA surrounding the response process and performance?

These non-technological and, in many cases, less- recognized business processes, structure, and cultural challenges impact security control in the long run. While these examples are the tip of the iceberg, it is essential to create a holistic and continuous process improving program within the organization to continue to ask, "How could our security culture be improved?"

Security Culture in IT Environments

Unlike OT, the recognition of the need for technologies is well-defined in IT as the mission, and make-up of business systems revolves around moving data by information technology teams. For example, starting with asset inventory and visibility, this is a commodity product set for the IT side of the house. There are many asset management vendors from which to choose, and a skilled IT team can quickly adopt these tools. The process of selecting technology may be influenced by an IT centric process. Cultural changes may be found that would better fit the selection of complementary products on the OT side. Asset Inventory, Vulnerability, and Risk Management are more challenging in OT due to the nature of the technology and topology. The personnel are

typically engineers that specialize in the process and not necessarily the tool (systems) with how they interact with the operations of moving molecules. The owners of OT assets have a different mission focus from IT owners, and their training is not necessarily one that includes cyber security studies. The creation of a culture of security must take these different mindsets into account and use relatable tactics to change behavior.

Culture Convergence: IT and OT

Unlike the typical IT categories of Confidentiality, Integrity, and Availability (CIA) or Identify, Protect, Detect, Respond, and Recover on the OT side, taking a risk-based approach may speak directly to the engineering resource owners by using critical key metrics like:

- Life, Health, Safety
- Impact on Production Capacity and Efficiency
- Maximum Tolerable Downtime (MTD)
- Mean Time to Recovery (MTR)

This tailored approach for IT and OT will drive the answers to, “Why should I care about security?” The organization will want to give the collective team a chance for success. While looking critically at the business process for assigning tasks across groups, subtle changes may become apparent when viewed through a security lens. While system “ownership” must remain bifurcated due to inherent operationally driven needs, the IT/Security/OT teams must all work in lockstep, as if tied at the ankles, to address critical vulnerabilities, potential security events, and incident response/recovery. Speed and efficiency are paramount when it comes to security events, malware, or possible breach response.

These are only two aspects of creating a security culture but serve as an excellent example of why there is more to changing behavior than simple information sharing. Many more areas of business in OT and non-OT environments will also need to be considered in the Security culture program, but every aspect will require top-down support to change the status quo. Creating a security culture is vital to any organization to augment the security technology investments but is indispensable to an OT operator’s survival in the fast-paced breach response process.