Aligning Enterprise Technology Orchestration and InfoSec

What employees need to know

TABLE OF CONTENTS:

One of the most challenging tasks facing IT and ITAM teams today is ensuring that all employees in their organizations understand how Information Security (IS) is a crucial part of everyone's job in an enterprise. Thinking and talking about IS for a non-technical audience can be a tough sell (until they've been victimized by it). Everyone is normally focused on their (non-security) job and security considerations, which can be pretty granular and inconvenient, often take a back seat. That said, the best line of defense against security breaches in an IT environment remains employee awareness, participation, and a clear understanding of the disposition of assets. According to one survey published in InfoSecurity magazine, 90% of data breaches in the United Kingdom were caused by employee error. [1]

This White Paper will cover why IS is such a critical component of Enterprise Technology Orchestration (ETO) and how IT teams can leverage ETO to facilitate improved IS. Bottom line - IS (similar to ETO) is part of "growing up" as a company. Teams that can understand the importance of IS and adopt good security practices across the product lifecycle will not only reduce the likelihood of catastrophic breaches and loss of customer records, but also streamline sales processes and improve internal communication. For these and other reasons, a robust IS program tied to Enterprise Technology Orchestration is essential to scaling and securing the modern enterprise and protecting the modern IT Estate. This White Paper provides a framework for how to think about Information Security in the context of ETO and provides key elements that can be repurposed for education and policy construction.

Section 1: Why Information Security is So Important

In the very near future, the vast majority of B2B, B2C, and C2C interactions will take place in digital forms. Internal business processes are rapidly moving to digital formats. This process of digital transformation, well underway previously, has been put on overdrive by the pandemic. This means that the majority of business activities will be more exposed to IS concerns and potentially exposed to online attacks. Indeed, this has already happened. In the 2020 VMWare Carbon Black Modern Bank Heists Report, COVID drove a 238% increase in attacks on financial institutions.[2]

> "
> **Protecting customer data across multiple devices is crucial to our ability to stay in business.**
> "

Today sophisticated hacking groups behave like multi-national corporations and state-sponsored Advanced Persistent Threat (APT) groups operate under the auspices of rogue governments beyond the jurisdiction of most law enforcement. Businesses that fail to protect their digital assets and customer data face nasty financial penalties under a growing list of laws at the international, federal and state levels. Fines for alleged failures in IS are now ranging into the hundreds of millions with the largest topping $200 million levied against British Airways.[3]

The upshot? Everything is going digital. And the risks have never been greater. While the overarching importance of IS is increasingly obvious, IT Teams educating employees and partners should break down the specific details of why IS is important. A basic list might include:

- Protecting customer data across multiple devices is crucial to our ability to stay in business
- Proper security processes and attestations are necessary to pass certifications such as SOC2 and/or CCPA
- Proper IS allows engagement with larger customers for bigger deals

[1] https://www.infosecurity-magazine.com/news/90-data-breaches-human-error/
[2] https://www.zdnet.com/article/covid-19-blamed-for-238-surge-in-cyberattacks-against-banks/
[3] https://www.bbc.co.uk/news/business-48905907

- Failure to secure company assets and their associated data can result in large fines and reputational damage
- Public IT failures can adversely impact an enterprise's ability to win contracts, and every day the potential number of failure points increases

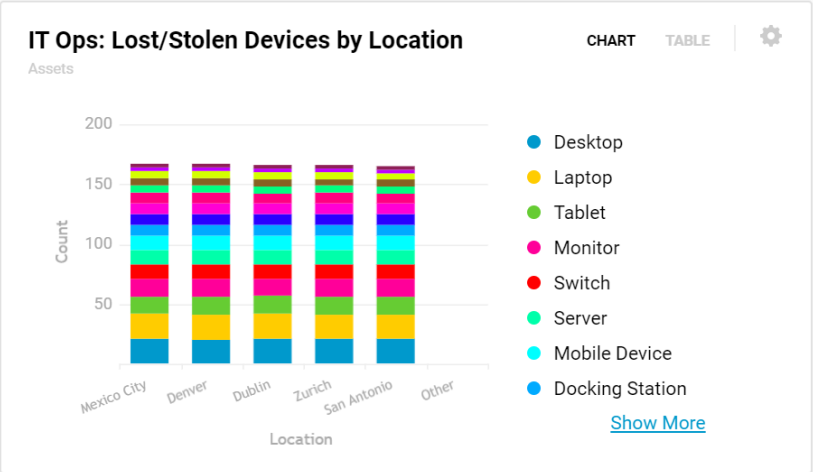
As mentioned previously, the only way to maintain proper IS is to ensure that all employees do their part to protect company assets against digital attacks. To guard against IS failures, every employee at an enterprise must:

- Understand their responsibilities in the areas of information security and privacy
- Understand the nature of emerging threats as it relates to their roles and the IT infrastructure under their control
- Recognize common threats to IT assets (broadly defined) and know how to protect them
- Understand the status and disposition of assets (where the data lives) in real-time
- Identify where to locate information security resources across a broad range of devices

Section 2: What Is Information Security?

Information Security is the protection of information and information systems (assets and the networks on which they run) from unauthorized access, use, disclosure, disruption, modification, or destruction. IT asset management teams and IT security teams must cooperate to structure and deploy proper Information Security practices and controls across an enterprise to sufficiently mitigate risk across any data-centric device or process.

Why is IS necessary? The practice of IS provides confidentiality, integrity, and availability of digital systems and maintains trust in those systems. IS is achieved through implementing technical, management, and operational measures designed to protect the confidentiality, availability, and integrity of information. The goal of



> "Proper Information Security can assure the reliability and accuracy of digital and IT resources."

an IS education and mitigation program is to understand, manage, and reduce the risk to information under the control of the organization.

To add detail, the core elements of protecting information are as follows:

- **CONFIDENTIALITY:** Protecting information on a device or in the cloud from unauthorized disclosure
- **AVAILABILITY:** Defending information systems and resources from malicious, unauthorized users to ensure accessibility by authorized users
- **INTEGRITY:** Assuring the reliability and accuracy of digital and IT resources
- **RISK MANAGEMENT:** The process of identifying and prioritizing threats and vulnerabilities to IT assets, and establishing defensible and acceptable controls to reduce the likelihood of a security breach or violation
- **CONTROLS:** countermeasures to avoid, mitigate, or minimize security risks

Controls is the term of art for IT security teams but it is not necessarily technological in nature. There are three types of controls to implement proper Information Security. Each is different but equally important.

- **MANAGEMENT CONTROLS** involve policy or procedures to manage risk and information system security.
- **OPERATIONAL CONTROLS** rely on people to perform certain actions to ensure security.
- **TECHNICAL CONTROLS** are primarily implemented and executed through mechanisms contained in the hardware, software, or firmware of the information system.

Management Controls: creating policies and procedures optimized for Information Security

The first step in creating an effective Information Security practice is to decide on policies and procedures that codify the basic "rules of the road". The policies must be available for humans to read and understand (including non-technical employees) but should also be programmatically addressable so security systems and IETO platforms can read and enforce security policies. In this sense, policies and procedures span human behaviors and technology solutions for IT security. An example of this might be policies for accessing corporate networks from outside the perimeter. The stated policy may be that users can only access corporate networks via VDI over a VPN. This policy can be enforced by endpoint protection

software (like Tanium), by ETO platforms (like Oomnitza) or by human actors who are instructed not to access sensitive corporate networks without these basic controls in place.

Operational controls: employee actions to improve Information Security

Operational controls involve human actors understanding the right behaviors when interacting with IT assets, and leveraging those behaviors to mitigate risk. Implementation of proper operational controls relies on a clear understanding of required policies and procedures. To assure this, IT security teams must regularly train on policies and all other employees must receive security training on a range of topics, but contextualized to the devices they use on a regular basis (behavior on a company-owned laptop will be different than that for an employee-owned mobile device, for example). Ideally the IT security team will create exercises or even games to transform operational control education from reading and quizzes to real-world drills and exercises.

Technical controls: applying technology for Information Security

Technical controls are deployed to implement Information Security policies as it relates to managing the IT portfolio and protecting the assets within it. These might include firewalls, anti-virus, malware detection, intrusion detection, digital loss protection, and more. Modern Infosec practices also incorporate prioritization and coordination tools including SIEM (Security Information and Event Management), SOAR (Security, Orchestration, Automation, and Response platform), and vulnerability management. Controls and coordination platforms can also deliver important up-to-date feeds of shared threat intelligence to mitigate risks against novel threats.

Section 3: How to Combat Cyber Attacks

Stopping cyberattacks requires preparation, awareness, and teamwork. Clear communication from security teams to the rest of the company is crucial. Likewise, the willingness of employees who are not in IT security or IT to report anomalies that may indicate an attack is underway is critical; often the employees are the first-line defense against these attacks. Their timely warnings save companies billions of dollars in damages each year.

There are some basic rules that all employees and organizations should follow including:

These all may seem obvious but you would be surprised how often employees attempt to circumvent these basic guidelines. AV software may slow down their machine. They may avoid patches out of fear that it will require them to take their machines offline. They may choose not to encrypt devices because they fear they will be locked out permanently and lose data should they forget their password or their password expires. Employees may share passwords for shared services, not realizing that people frequently reuse the same password for multiple purposes. So even these seemingly obvious steps require reinforcement and constant checking.

Beyond these policies, some areas merit deeper explanation.

Practice secure communications

Communications via email, text, and chat are the most frequent way that key information is exfiltrated and cyberattacks gain a foothold inside the perimeter. It is critical to be aware of and follow communications policies and procedures as outlined in an enterprise's Information Security Policy.

Any Secure Communications Policy should mandate the following:

- **Never use personal,** third-party email addresses to send company information to anyone, including other employees. Third-party email is far less secure and cannot be easily monitored by company IT staff.
- **Never download,** save or execute untrusted or suspicious email attachments through personal, third-party email addresses on company-owned devices. This is particularly challenging in the era of Bring Your Own Device (BYOD) and employees may resist the requirement to keep work and personal digital communications firewalled but using personal emails to plant malware or other executables on corporate devices is a popular tactic.
- **Be cautious** when browsing the web and do not download, save, or execute untrusted or suspicious software or e-mail attachments. Attachments are a favorite vector for installing malware on company devices and often hackers use social engineering and common file types to obfuscate the danger of an attachment.

- **Never use** another employee's credentials to access a system. If those credentials are copied or sniffed, then hackers may gain access to sensitive systems. In social engineering attacks, hackers impersonating other employees often ask to borrow credentials to access systems.
- **Internal resources** should only be accessed from company-owned devices, unless specifically exempt in the Information Security Policy. This policy, however, may be changing as more and more enterprises adopt Zero Trust authentication systems which continuously validate identity and are designed to allow more fluid, secure

Mobile device loss and theft

While hackers attempting remote attacks are the biggest threat, a large number of breaches occur because of loss or theft of mobile devices. Mobile device loss is even more risky today as many authentication systems are set up to use texts to phones as the second piece of 2-Factor Authentication systems. So anyone possessing the phone is more likely to be able to break through normally secure 2FA defenses.

Here is how employees and ETOteams can combat mobile device loss and theft:

- Never leave laptops, cell phones, or other mobile devices unattended – especially when traveling.
- When away from your desk, use a computer lock for your laptop or place it in a locked cabinet.
- Do not let family members borrow your devices, particularly teenagers Mobile devices that contain PII must be encrypted.
- Completely shut down your laptop while in transit to enable encryption.
- Have a clear, real-time view into the status and disposition of all assets, including accessories.
- Track usage and act quickly on anomalies (logging in at odd hours or from odd locations)
- Report lost or stolen devices immediately.

Social Engineering

Social engineering is classically defined as the art of manipulating and exploiting human behavior to gain unauthorized access to systems and information for fraudulent or criminal purposes. This is, unfortunately, fairly common. Social engineering attacks are more common and more successful than computer hacking attacks against the network. An example of a massively damaging social engineering attack was the recent attack against Twitter where hackers gained access to internal tools and tweeted requests for bitcoins from prominent accounts like Elon Musk and Joe Biden. In social engineering attacks, criminals leverage natural human instincts like trust or the desire to help to manipulate people to divulge valuable information such as passwords, secret system design information, and internal intelligence about how processes work. With social engineering, criminals can bypass network firewalls and building access systems to steal data and disrupt operations with a successful social engineering attack.

Here are some basic guidelines on how to combat social engineering:

- When someone familiar asks for help you can ask them for other pieces of information that they likely do not know (e.g. a favorite restaurant or some other piece of information that they have).
- Be cautious of sharing personal information publicly on social media sites like Facebook.
- Be aware of favorite social engineering pressure tactics - creating a sense of crisis and urgency, pleading for help, appealing to strong emotions, showing strong emotions.
- Be aware that social engineering attacks may build up over time through ongoing conversations with compromised accounts.
- Always put in place 2-Factor Authentication and, if possible, add additional factors such as voice passwords or other checkpoints
- Be careful with new friend requests on social media, particularly from someone who has no obvious connection to you.

Phishing (and Related Attacks Like Spearphishing and Whaling)

Phishing is an attempt to obtain personal information such as passwords, usernames, and credit card numbers by masquerading as a trustworthy entity in an electronic communication. This is a type of social engineering attack. Spearphishing is highly-personalized phishing attacks that refer to other people the target knows and appear to be legitimate. The attack on senior Democratic Party officials in the United States that yielded access to party email servers was the result of a spearphishing, Whaling is a phishing attack directed at senior executives in an attempt to gain access to high-value information like sensitive customer data or proprietary business information. A successful attack can be devastating because it involves high-level access to an organization's network systems. Related to whaling attacks are business email compromise attacks where an attacker seeks to gain access to business emails through rerouting legitimate emails or encouraging executives or finance professionals to respond to an address that is very similar to a legitimate address. These types of attacks often target bank fraud and can result in millions of dollars in damage.

Here are some basic tips to share for combating Phishing, Spearphishing and Whaling Scams:

- Do not respond to email or text messages that ask for personal information like credit card numbers, Social Security numbers, passwords, etc. Particularly if it comes from a corporate authority figure like a CEO. Forward those emails to your IT Security team
- Do not click on suspicious links provided in email or text messages. The link could be to a fake or spoof site, which looks legitimate but is set up by criminals to steal your information. Link shorteners are often used for this, as well.
- Closely study the email address of the sender if an email seems suspicious or asks you to do something out of the ordinary. Often the email address is designed to look legitimate but is not.

The same is true for site URLs.

- Review financial statements at least once a month for unauthorized charges.

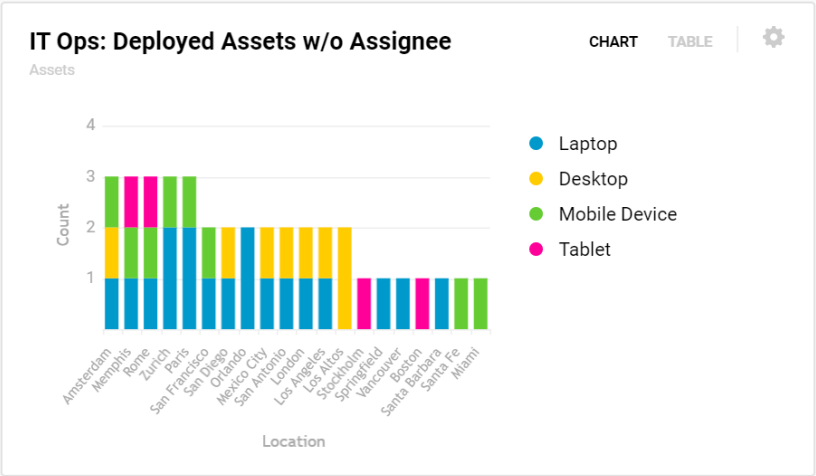
Section 4: Incident response

The final consideration in Information Security training is how to respond in case of an attack or incident. An incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits. An incident generally means sufficient probable cause to fear that a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies is underway or has occurred.

Examples of incidents

Here is a list of examples that might indicate an incident has occurred and should be reported:

- Loss, damage, theft, or improper disposal of company equipment, documents, or files
- Disclosure of PII or other proprietary information to individuals who are not authorized.
- Viruses, phishing emails, social engineering attacks
- Breaches of physical security
- Uncontrolled systems changes (bypassing change controls)
- Access violations (bypassing access controls)
- Malfunctions of software or hardware
- Unauthorized activity on software, equipment or devices (e.g., hacking, malware)
- Breach of a system, service or network
- Possible exploitation of a security vulnerability or weakness
- Ineffective security controls
- Breach of information integrity, confidentiality or availability expectations
- Human errors (innocent or otherwise)
- Non–compliance with policies or standards



When and how to report an incident

ETO and IT security teams are constantly looking for signs of incidents and have a detailed understanding of reporting requirements and procedures. Non-technical employees tend to have less understanding and exposure. They should be encouraged to report any suspicious incidents or behaviors and communications immediately upon receipt. They should also be told not to worry about false positives and that their vigilance is key to keeping the company secure. IT security and IT should create easy channels for reporting in Slack, MicrosoftTeams, via email, and with dedicated phone numbers. Every employee should have easy access to these communications channels on the company intranet or other common online locations.

Conclusion

The management of data, and the IT assets on which it resides, has never been more exposed than it is today. With the sudden acceleration of digital transformation driven by the pandemic, combined with a significant increase in devices (IoT) and a steady move to the cloud, the IT estate has a far greater attack surface. An integrated, holistic view of all IT assets, where they are, and who they're associated with is critical for the success of today's modern enterprise.

About Oomnitza

Oomnitza is an agentless enterprise technology orchestration solution for digital business. By orchestrating technology assets data from siloed systems into a single pane of glass, our customers are able to optimize their technology spend, automate their governance processes to meet compliance and auditing requirements, protect from security risks, and ensure a great employee experience. Oomnitza is headquartered in San Francisco

www.oomnitza.com

2/21