Four Step Guide to Creating an Internal Culture of Security

ABOUT EZE CASTLE INTEGRATION
Eze Castle Integration is the leading provider of IT solutions and private cloud services to more than 650 alternative investment firms worldwide, including more than 100 firms with $1 billion or more in assets under management. The company’s products and services include Private Cloud Services, Technology Consulting, Outsourced IT Support, Project & Technology Management, Professional Services, Telecommunications, Voice over IP, Business Continuity Planning and Disaster Recovery, Archiving, Storage, Colocation and Internet Service.

TABLE OF CONTENTS

WHERE THE VULNERABILITIES ARE ................................................................. 3

WHAT IS A SECURITY-ORIENTED CULTURE? .................................................. 4

1. CREATE A COMPUTER INCIDENT RESPONSE TEAM .................................... 5

2. DEFINE YOUR TERMS ................................................................................. 6

3. DELIVER COMPREHENSIVE TRAINING ...................................................... 6

4. REMEMBER THE INTERNAL CULTURE REACHES OUT EXTERNALLY ............ 7

ABOUT EZE CASTLE INTEGRATION .................................................................... 9
WHERE THE VULNERABILITIES ARE

It’s 3:40 on a Friday afternoon, and an urgent email hits a back-office employee’s inbox. As the employee scrambles to get ready for the market-close and head off to a three-day weekend, it looks like the portfolio manager for a major client needs him to wire $125,000 to a bank in Grand Cayman.

His colleagues are tied up with other matters, and, since he’s eager to be responsive to this important client’s request, he follows the wire instructions in the email to complete the transfer – with just a few minutes to spare.

Bad move.

Unfortunately, in his haste to complete the transaction request, the employee neglected to see the carefully crafted and well-disguised typo in the domain name of the email address. That message wasn’t from a portfolio manager. It was from a hacker in Eastern Europe cleverly concealing his identity. Just minutes later, after the theft was detected, the employee called the bank to reverse the wire – but the money was already “two hops” away, never to be seen again.

The reality is, the Hollywood stereotypes of cellar-dwelling, over-caffeinated nerds devising new ways to slip into corporate networks are fading away. Today, more often than not, the nightmare scenarios involve “social engineering” and sophisticated operations involving dozens or hundreds of “employees” set up in office parks who prey on human weaknesses, not computer weaknesses. That’s because, even while the sophistication of perimeter security and vigilant monitoring increase, the greatest vulnerability, sadly, remains the people who use your IT systems to conduct transactions and access sensitive data.

This fictitious investment firm didn’t need more firewalls, more passwords, or more encryption. What it needed was an internal culture of security, an ongoing, organization-wide commitment to defining and adhering to careful, thoughtful policies that reduce or eliminate “people vulnerabilities” through assessments, awareness, and education.

The following white paper outlines the characteristics of an internal culture of security and how your firm can pursue and achieve that crucial mindset.

Phish Finding: Steps to Prevent Being Duped

1. Multiple points of verification
2. Segregation of duties
3. URL examination
4. Slow down
**What is a Security-Oriented Culture?**

It’s just possible you had a friendly lunch with the person who’s the biggest threat to your firm’s information security. That’s because Kelsey in accounting or Matt in marketing may be unknowing conduits for the true cybercriminals.

As our previous scenario shows, sometimes all of the firewalls in the world won’t stop some of the most damaging attacks. In many instances, employees are “holding the door open” to criminals or inadvertently “leaving the keys out.” At other times, disgruntled employees act with more malicious intent.

So how do we strengthen these people-centric security vulnerabilities? We must create a security-centric culture. And, above all else, that needs to start from the very top of the firm (people who, ironically, due to the volume and sensitivity of the information they access and the distractions their fast-paced lives encounter, can sometimes represent the greatest source of vulnerabilities to information security). It’s essential that they visibly and fully commit their unwavering support to your efforts to improve security.

That doesn’t mean transforming your offices into a fortress, nor instilling any sense of paranoia in Kelsey, Matt, or the rest of your employees. However, at its essence, it does mean creating and sustaining a heightened level of awareness.

---

**Identifying Security Threats Created by Employees**

<table>
<thead>
<tr>
<th>Unintentional Threats</th>
<th>Intentional Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>* Weak or Shared Passwords</td>
<td>* Disgruntled Employee</td>
</tr>
<tr>
<td>* Unsecure Equipment: Laptops, mobile devices, computer room, backup tapes, USB drives</td>
<td>* Monetary Gain</td>
</tr>
<tr>
<td>* Improper Disposal of Hard Copy Documentation</td>
<td>* Convenience</td>
</tr>
<tr>
<td>* Visitor Access to the Network</td>
<td>* Trade Secrets</td>
</tr>
<tr>
<td>* Employee Curiosity</td>
<td></td>
</tr>
<tr>
<td>* Lack of Knowledge or Security Awareness Training</td>
<td></td>
</tr>
<tr>
<td>* Employees Being Too Busy/Rushed</td>
<td></td>
</tr>
</tbody>
</table>

*In a PwC 2015 global state of information security survey, 72% of surveyed respondents attributed security incidents to either current or former employees.*
1. CREATE A COMPUTER INCIDENT RESPONSE TEAM

Your first step is to find the right people who can oversee your information-security policies and be part of a “Computer Incident Response Team.” Although IT professionals are responsible for overseeing and maintaining your computing infrastructure, you also need business users to play a central role in your security initiatives. After all, they’re the ones who use these resources – and the ones who can represent the biggest vulnerabilities and risks. While the team’s responsibilities can vary, many CIRTs are active in several key areas:

- **Create a Plan** – Development and writing of an information security plan, and working closely with their peers out in the various departments to implement and maintain the plan.

- **Create Training Programs** – This operationalizes the firm’s security plans and policies.

- **Respond to Incidents** – Business users can add valuable insights, assess the business impact of breaches, determine who must be notified, and more.

- **Communicate with Peers** – CIRT team members spread the word to colleagues and keep security top-of-mind. They also help coworkers self-assess security risks and encourage constant awareness.

**Define Technical Safeguards and Responses**

With a business perspective, the CIRT team can help IT define the technical restrictions that should be in place – everything from encryption for mobile devices to screen-lock policies, USB usage, antivirus scanning, spam filtering, password policies, penetration tests, audits, and much more. These are matters that should not be in the sole jurisdiction of technical experts.

In the event of a breach, your CIRT can manage and facilitate the response that’s needed after assessing the impact of an incident. That can encompass working with internal stakeholders and notifying regulators and government officials as required by law. Your business people – not the IT team – best know the value of that data, and they’re in the best position to define the response.
2. **Define Your Terms**

Before you can secure your confidential information, it’s important to define exactly what you mean – and ensure everyone in your organization is literally and figuratively on the same page.

Many firms create a 10-20-page written information security plan that formalizes the definitions and policies that govern the creation, access, and deletion of confidential information and computing services. That can be everything from a definition of personally identifiable information (PII), a description of user access privileges and roles, or policies regarding USB thumb-drives. What matters is that you’ve explicitly and unambiguously documented all aspects of your company’s at-risk assets and services.

While the plan should be comprehensive, avoid getting bogged down in “tech speak.” Users don’t want jargon – they want to know if they’re protected. They want to know the implications of their actions (“If I read this on a mobile phone, am I creating a security vulnerability?” “Can I download this onto a USB drive?”)

A multi-disciplinary cross-functional team often works best in these efforts. Often, a simple one-page summary of employee guidelines is enough to shore up most of the important gaps quickly, while continuing to increase company-wide awareness.

3. **Deliver Comprehensive Training**

“Operationalizing the culture” – it’s a mouthful to say, but it’s still important to recognize. All of the documents, committees, and meetings won’t have any meaningful impact if the proper security practices don’t spread quickly and uniformly across the organization. And the way that starts to happen is through systemic and comprehensive training practices.

Vendors can help you develop the right curriculum – tailored to your business’s unique needs, preferences, and policies.

---

**Malice, not Mistake: The Disgruntled Employee**

Sometimes, security lapses aren’t caused by mistakes or careless oversights. They’re the deliberate result of disgruntled employees – people who have access to confidential information and sensitive resources.

Here are some steps you can take to prevent or mitigate the damage:

* Lock USB ports to prevent data copying
* Implement segregation of duties
* Create Access Control Policies based on a “need-to-know” basis
* Utilize file system auditing and alerting software tools
* Perform background and credit checks during the hiring process
* Closely monitor lower-performing employees
* Have an Incident Response Plan
• **Face to Face** - Many organizations find that face-to-face, instructor-led, hands-on training is the best way to instill the security culture. The emphasis needn’t be (and shouldn’t be) on the bits-and-bytes with a lot of tech-speak. Instead, focus on what business users need to know to keep IT resources secure and protected. These scheduled sessions – which should last no more than 30-60 minutes – let people learn visually and practically and send a strong message about the importance of security.

• **Video Refreshers** – When employees have quick questions or when face-to-face sessions aren’t practical, on-demand video lessons can fill an important gap. Start by taping your face-to-face sessions and edit them into quick five-minute segments. A library of key topics can be a great resource.

• **Start Early** – Underscoring the importance of security, many employers are making security training part of their onboarding process – and asking employees to start training before their date of hire. Make sure new hires recognize their responsibilities from day one.

• **Keep it Going** – Make sure the awareness doesn’t stop with the training. Regular newsletters about data security are a good strategy. Periodic reminders from top managers can also reinforce your security-oriented culture. Update your teams about new and emerging threat strategies and sources.

4. **Remember the Internal Culture Reaches Out Externally**

Even when you have locked down your internal systems, implemented best-practices policies and procedures, and trained your employees to think “security first,” there’s still more work to do, culture-wise.

• **Assess Third-Party Risks** – Perhaps the weakest link in the security chain is one you have little (or no) control over: the performance of your partners. For example, have you analyzed the security practices of your strategic business partners? Does your payroll provider follow stringent practices that eliminate openings for hackers and other bad actors? Are your clearing house and transfer agents taking the right steps to prevent intrusions? After all, when you tightly integrate with their systems and share data securely, you’re still vulnerable to whatever keystroke loggers enter your environment. Or are those elite access credentials getting stolen elsewhere – and used to access your databases?

• **Regulatory Risks** – Following the right security practices will enable you to achieve clean audits from industry and government regulators. What you do inside will greatly affect your external reputation.

• **Personal Email** – Even if your employee is following all of your processes and practices with work-related email, you could still be vulnerable if her private, personal email is breached or corrupted. That can unintentionally open a back door to your network environment. And that means security vigilance must extend from professional to personal domains.
CONCLUSION

Having proper perimeter defenses and rigid security controls are, of course, non-negotiable requirements for any financial services firm. But the new front lines in corporate IT security aren’t technical – they’re people. By developing an internal culture of security, the organization does far more than deploy and configure bits and bytes. It commits to defining and following thoughtful, far-ranging policies to eliminate the needless internal vulnerabilities that often go unrecognized.

From a properly trained and staffed computer incident response team to carefully defined policies and procedures to complete training, financial services firms can take simple but important steps to prevent breaches, strengthen security, improve regulatory compliance, and increase customer confidence. For more information, visit www.eci.com.
ABOUT EZE CASTLE INTEGRATION

Eze Castle Integration is the leading provider of IT solutions and private cloud services to more than 650 alternative investment firms worldwide, including more than 100 firms with $1 billion or more in assets under management. We provide one global financial cloud platform, Eze Private Cloud, that is complimented by exceptional service and operational excellence.

We also provide clients Cybersecurity solutions (Eze ATP) and assist in developing Written Information Security Policies (WISP) and Business Continuity Plans (BCP).

To learn more about Eze Castle Integration, contact us at 800-752-1382 or visit www.eci.com.

Complete Managed IT — Software as a Service

Eze Managed Suite is a fully managed IT solution that provides flexibility and simplified IT operations. The hosted IT solution combines a robust, highly secure private infrastructure via the Eze Private Cloud with key business applications and professional IT management.

Cybersecurity: Eze Active Threat Prevention (Eze ATP)

Eze Active Threat Protection is a fully managed cyber security service for protection against advanced persistent threats through intrusion detection, intrusion prevention and security incident response.

Written Information Security Policies + Business Continuity Plans

Eze Information Security Policies center on the development, implementation and audits of written information security plans and procedures for hedge funds, family offices and investment management firms.

Eze’s Business Continuity Planning Services extend beyond technology to focus on critical operations and processes that firms must have available if a disaster strikes. Our Eze BCP consultants are certified experts in business continuity planning and possess deep knowledge of the unique operations of financial services firms.