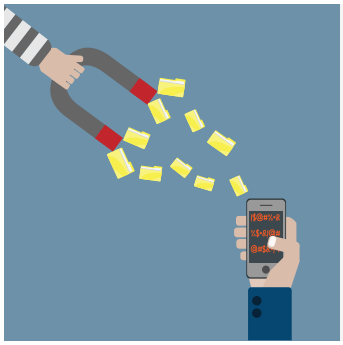
The Enemy Within: Insiders are still the weakest link in your data security chain

ABSOLUTE™

Whitepaper

The Enemy Within: Insiders are still the weakest link in your data security chain

With companies embracing mobility to maintain competitive advantage in the digital era, information security threats have increased exponentially. User-friendly technologies such as mobile devices, mobile apps, and cloud storage are often hacker-friendly too, creating opportunities for cybercriminals to covertly infiltrate company data. This opens the door to data loss, reputational damage, loss of proprietary information – not to mention the associated regulatory penalties and potential legal fees. IT bears the brunt of responsibility for information security, yet according to Forrester, internal incidents top the list of security breach causes in 2014.



"59% of US employees consider the value of the corporate data on their phone to be less than $500."

The digital, mobile era matured so quickly that data security strategies have barely kept pace with the change. At the center of this transformation is the humble employee. Employees can now access company data from any location, on the device of their choice. While policies such as bring your own device (BYOD) are commonplace, few employees take the time to read about the stance of their company on data usage and even fewer take any responsibility for data security. Interestingly, a study commissioned by Absolute found that 59% of US employees consider the value of the corporate data on their phone to be less than $500 (Absolute 2013).

Despite this glaring, human-shaped hole in information security, most organizations fail to provide regular security awareness training to their employees. According to a recent Forrester study, only 37% of North American and European workforces indicated that they received training on how to stay secure at work, and only 53% said they were aware of corporate security policies. Yet, in 2014, 42% of internal security incidents were due to inadvertent misuse or an accident (Forrester 2014).

The media is littered with data breach headlines as the frequency of cybercrime incidents soars. Cybercrime is lucrative and the threats are often advanced and persistent. As a result, over half of all security and risk professionals admit to being overwhelmed by the number of attack vectors (Shey and Mak 2014) and they lack confidence in the ability of their organization to protect data in such a tumultuous environment.

A layered approach to security that includes firewalls, SSL protocols, encryption, and Persistence® technology is widely recommended to safeguard against cybercrime. Yet there is another layer of defence that can be added – your employees. Forrester recommends that organizations focus on people, as well as technology, when considering a data security strategy. Astute employees can become a first line of defense against attack, rather than a chink in the armor. Layered security technology, diligent employees, and a collaborative approach to dealing with cybercrime will ensure that your data remains secure, despite the challenges of the digital era. Follow these five steps to foster a conscientious data security environment in your organization.

1. EDUCATE EMPLOYEES TO BE YOUR FIRST LINE OF DEFENCE

Your employees have access to company data but don't always know or understand data use policies. According to Forrester (2014), 49% of North American and European information workers are not aware of or do not understand the policies in place that are specific to data use inside their company and only 56% say they actually follow security policies in general.

This is not the fault of the employees. It has been argued that many organizations have overly complex data classifications or ineffective data use policies (Shey and Mak 2014). Organizations should define their data clearly and assign definitive roles for data creators, owners, users, and auditors.

Educating employees greatly reduces the risk of vulnerabilities caused by human error. Make sure all staff members have access to proper training, even on things that seem rudimentary to an IT professional, such as remembering to log off their

5 ways to foster a data security environment

- Educate employees to be your first line of defence
- Conduct random security tests to keep employees on their toes
- Collaborate with associates and form a cybersecurity alliance
- Build a security fortress and protect it with a persistent watchdog
- Form an actionable crisis plan

workstation when they leave their desk or keeping their passwords secret.

Employees can be viewed as potential points of failure or potential security checkpoints. With proper training and clear communication of data use policy, employees can become the first line of defense against cybercrime

2. CONDUCT RANDOM SECURITY TESTS TO KEEP EMPLOYEES ON THEIR TOES

According to Forrester (2014), 42% of external attacks involved some type of user interaction (watering hole attack, phishing, malicious link, or email attachment). The best way to ensure that employee training is effective is to conduct frequent security tests (Lindros and Tittel 2014). Gamify security audits by keeping a leaderboard to maintain employee engagement. Examples of such tests include:

- **Spot quizzes:** Administer random quizzes several times per year and vary the questions so employees don't become familiar with a pattern or share their responses. Scores should be public to foster a competitive environment. Employees who perform poorly should receive further training and receive more frequent testing until they achieve a higher standard.
- **Workspace checks:** Employees can become complacent with information that they handle routinely. Check employee desks for documents or notes that contain confidential information. Check that devices in the area are locked if left unattended and check the area around devices for password reminders or encryption keys on post-it notes, etc.
- **Honey traps:** Leave USB keys lying around public areas or post USB keys from false "marketers"to random employees. Place some code on the keys that will alert you when it is plugged in and allow you to identify the employee
- **Social experiments:** Hire a temporary employee or an actor to pose as a new staff member. Ask them to call on random employees, requesting confidential information such as login credentials or information in a non-public document. The employee/actor should have a credible story prepared about why he or she needs the information.
- **Simulated email attacks:** Phishing emails are disguised to come from a legitimate source but they contain links to malicious websites or attachments. These emails often fool typical users. Teach employees how to identify a suspicious URL before they click on it. Send phishing emails to random inboxes and monitor who clicks on them. The links can redirect to a webpage that informs the employee about the security test.

This type of regular testing is important to keep data security top-of-mind with employees. If these procedures are too onerous for your team to manage, there are third party consultants that can manage security testing on your behalf.

"42% of internal security incidents were due to inadvertent misuse or an accident."

3. COLLABORATE WITH ASSOCIATES AND FORM A CYBERSECURITY ALLIANCE

Employees are not the only company stakeholders that cause data security concerns. According to Forrester (2014), third parties and contractors have widened the attack surface. Cybercrime is becoming more advanced and criminals have moved on from targeting individual organizations to targeting entire networks of organizations. Trusted business partners can access systems without setting off any alarms - recent breaches at Home Depot and Dairy Queen were traced back to compromises at third party suppliers (Vinton 2014).

By forming cybersecurity alliances with your business partners and even with competitor companies, you can ensure that you have all of your bases covered, making it more difficult for cybercriminals to gain entry. By sharing experiences with peers, you can spot patterns quicker and share best practices on network and endpoint security and employee training.

4. BUILD A SECURITY FORTRESS AND PROTECT IT WITH A PERSISTENT WATCHDOG

Safeguarding your company data requires taking both a micro and a macro view of your security posture. ISO27001 compliance provides a useful framework for implementing ongoing security best practices and you should ensure that your technology providers follow the same high standards.

You can invest in the best firewalls, network access controls, encryption, and SIEM technologies on the market, but your endpoints are still in the hands of the employees. A recent Verizon study found that 71% of cybercriminals target user devices (Verizon 2014). With more employees working on the go, the endpoint has become one of the biggest threats to data security.

Persistence technology from Absolute acts as a watchdog over your endpoints and the sensitive data they contain. It offers IT a trusted lifeline to each device in their deployment, regardless of user or location. IT administrators can receive encryption status reports, monitor potentially suspicious devices, and remotely invoke pre-emptive or reactive security measures such as device freeze, data delete or data retrieval.

"Recent breaches at Home Depot and Dairy Queen were traced back to compromises at third party suppliers."

Persistence technology is embedded in the firmware of most computer, tablet, and smartphone devices at the factory. It is built to detect when the Absolute Data & Device Security (DDS) agent has been removed. If the agent is missing, Persistence will ensure it automatically reinstalls, even if the firmware is flashed, the device is re-imaged, the hard drive is replaced, or if a tablet or smartphone is wiped clean to factory settings. Absolute DDS also enables forensic functionality for confidential insight into internal criminal activity or non-compliance, as well as the investigation and recovery of stolen or lost devices. In fact, 80% of endpoint data breach scenarios can be mitigated with Absolute.

5. FORM AN ACTIONABLE CRISIS PLAN

Every organization is just one mistake away from a crisis. Build a cybercrime playbook filled with attack scenarios and response actions. Put escalation levels in place and decide how transparent you want to be about an attack.

A data breach will impact most departments in an organization, as well as any business associates that may be connected to the breach. It is important to establish a crisis management team with the heads of each department including public relations, human resources, IT, legal, and finance. Key stakeholders should provide relevant information pertaining to the incident. For example, in the case of a breach caused by a compromised device, IT can provide an audit log highlighting a device's security posture at the time of the breach. It is important to ensure that a detailed communications plan is in place and that employees are aware of how they should respond to questions about the breach.

THE FOUR A'S OF DATA PROTECTION

According to Chaudhary et al. (2012), the basic structure of data protection can be summed up in the Four A's:

- **Authentication** – Who is requesting access to data?
- **Authorization** – Do those individuals have permission to access the data?
- **Audit** – How is access to data monitored?
- **Administration** – How is data governance communicated throughout the organization?

Absolute can help you gain visibility into each of these areas and help you ensure that governance, risk management and compliance measures are in place. The unique persistence technology offers an important layer to any data security strategy and helps mitigate the risk of human error, rogue employees, and cybercrime. Absolute can help organizations plug the security holes created by mobility and human error.

REFERENCES

Absolute (2013) 2013 US Mobile Enterprise Risk Survey Summary Report. [Online] Available from: http://www.absolute.com/en/resources/research/mobile-enterprise-risk-us [Accessed 10 December 2014].

Chaudhary, R, Horwath, C., Del Giudice, M (2012) Have You Conducted A Data Protection Audit Lately? The FSA Times [Online] Available from: http://www.theiia.org/fsa/2011-features/have-you-conducted-a-data-protection-audit-lately/ [Accessed 10 December 2014].

Lindros, K and Tittel, E (2014) How to Test the Security Savvy of Your Staff. CIO Magazine. [Online] Available from: http://www.cio.com/article/2378559/data-breach/how-to-test-the-security-savvyof-your-staff.html [Accessed 10 December 2014].

Verizon (2014) The 2014 Data Breach Investigations Report (DBIR). [Online] Available from: http://www.verizonenterprise.com/DBIR/ [Accessed 10 December 2014].

Shey, H and Mak, K (2014) Understand The State Of Data Security And Privacy: 2014 To 2015. Forrester Inc. [01 December 2014].

Vinton, K (2014) Data Breach Bulletin. Forbes [Online] Available from: http://www.computerweekly.com/news/2240234281/Home-Depot-traces-credit-card-data-hack-to-supplier-compromise [Accessed 10 December 2014].