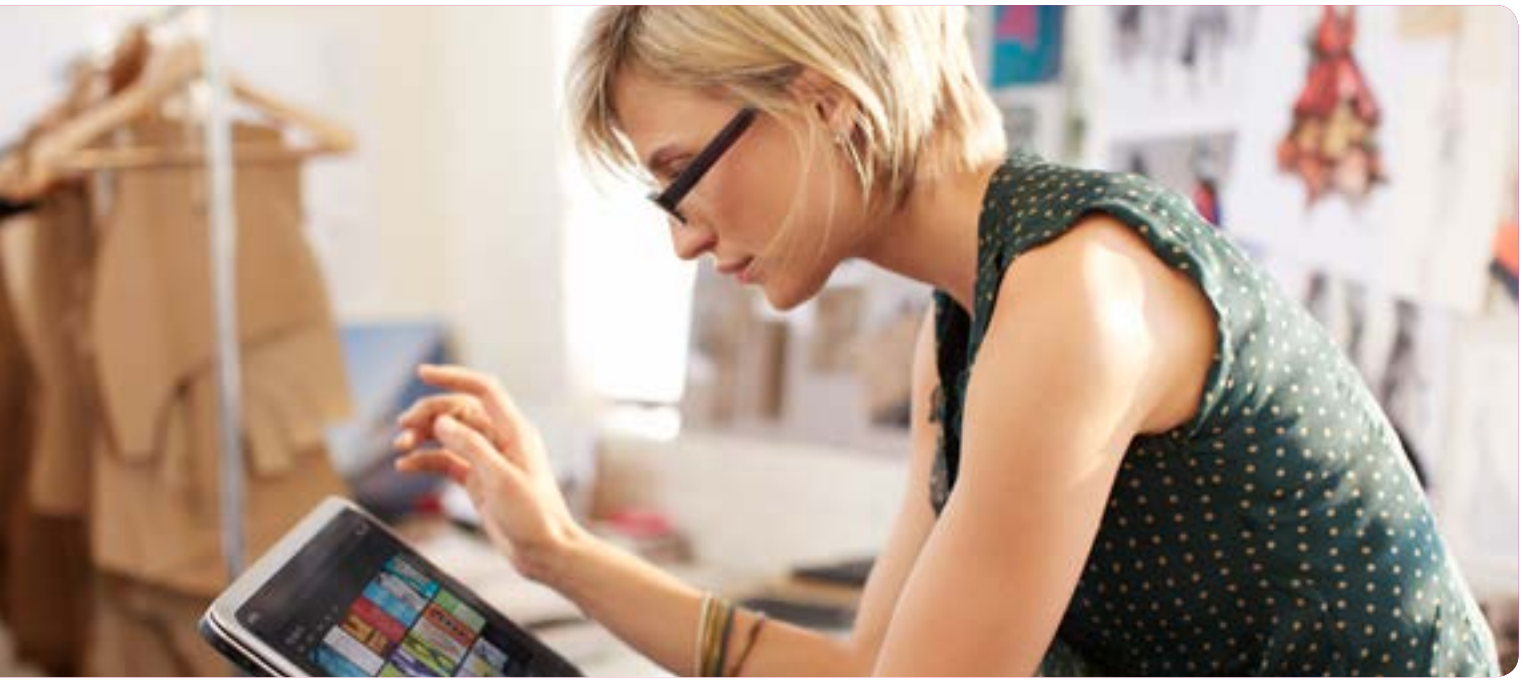
The Human Side of IT Security

In the effort to secure enterprise data, people can be assets, not liabilities



Winston Churchill once said, "All men make mistakes, but only wise men learn from their mistakes." Despite our best efforts, human beings are, and will always be, imperfect. And so too are the systems that human beings design and maintain, from governments to corporations to schools to hospitals. Of course, the same is true of IT security systems, which employ powerful technology, but in the end are only as strong as the people that use them.

The litany of infamous security breaches that have allowed hackers to steal millions of credit card numbers and consumer names and addresses from the largest retailers in the U.S. turns out to not be particularly sophisticated. In the aftermaths, we've learned that many of these companies' defenses were fully prepared with malware detection tools and that the technology did its job. If the tactics weren't that sophisticated and the defensive technology in place worked as intended, then how can we account for what happened?

It's come to light that a series of human errors are often in play — starting with successful targeted phishing attacks on employees that go undetected for weeks and give cybercriminals ample time to collect sensitive customer information from inside the payment systems, damaging the company's reputation and profits.

It is widely accepted today that human errors like this cause the lion's share of information security breaches around the world. In fact, one survey found that 70 percent of IT security breaches can be attributed to human elements.[i]

"Among the most common causes of data loss and security breaches are the vulnerabilities of an organization's employees," notes Chief Information Security Officer at Dell SecureWorks, Doug Steelman. "Companies can have plenty of security controls with abundant security instrumentation and keep their software up to date. Yet one click from an employee—uninformed about security policies or

> "Among the most common causes of data loss and security breaches are the vulnerabilities of an organization's employees."
>
> *Doug Steelman*
> *Chief Information Security Officer, Dell SecureWorks*

simply trying get the job done in the most expedient way possible—can inadvertently give access to threat actors with malicious intent, circumventing security technologies in place."

That is why forward-thinking companies are investing in more than just technology to shore up their IT defenses. They are working to educate, train, and cultivate a culture of security among the employees of their organizations. They are working to transform their people from security liabilities, to security assets, foot soldiers in the battle to secure the enterprise against an ever-changing threat landscape.

Creating a 'Culture of Security'

In today's hyper-connected world, data is the lifeblood of business. And that data includes billions of pieces of personally identifiable contact information, account numbers, healthcare patient records, trade secrets and a wide range of other sensitive material. The value of data increasingly relies on the ability for the right people—and only the right people—to access it wherever and whenever it's needed. To drive innovation and agility, organizations are adopting mobile, social, and cloud computing technologies at an accelerating rate. And these technologies are delivering data and applications beyond the reach of company firewalls and many traditional mechanisms of IT security.

Securing information everywhere it resides and everywhere it needs to go is a top priority. But even as they keep pace with increasingly sophisticated cybercrime techniques, IT security technologies are only as effective as the people who use them (or don't). A small sample of the myriad of human errors committed thousands, if not millions, of times each day include:

- Clicking on a malicious link in a seemingly innocent email
- Using a simple password or using the same password for both work applications and personal accounts
- Leaving a smartphone or laptop in a taxi or airport
- Uploading proprietary data to a public cloud service

Whether slip ups are made out of carelessness, ignorance or a well-intentioned attempt to get work done faster, the results can be equally damaging.

For organizations to truly secure their information, they need employees, partners and others with access to their data to understand, embrace and comply with well-articulated security policies and protocols. And those policies and the technology that enforces them must be easy to use. They cannot be barriers to productivity. Creating this "culture of security" requires a comprehensive, end-to-end strategy, tailored to the unique business requirements of each organization and supported by top management.

Addressing the human side

No technology provider can eliminate the possibility of human error. Dell's approach to security—based on simplicity, efficiency and agility—makes it easier for the business to manage rules and policies, and for end users to comply. At Dell, we see four fundamental solutions organizations can deploy to address the most common human behaviors that create security vulnerabilities:

- **Security awareness training** – a comprehensive and continual approach educates employees and changes their behavior regarding security
- **Identity and access management** – governs access to data, applications, and privileged accounts, providing the right people the right access without hindering productivity

- **Mobile and endpoint security** – protects desktops, laptops and other mobile endpoint systems from hackers, spyware, spam and viruses, as well as encrypts data, while maintaining user productivity

- **Network security** –protects networks while sustaining performance and enabling secure connections to corporate systems and data, monitoring for the most likely user-triggered security lapses

Security awareness training
Numerous studies state that anywhere from 91 to 95 percent of all security attacks begin with spear phishing emails or phone calls—attempts to trick individuals into providing security credentials or other information that can be used to circumvent defenses. Training users and raising awareness of these risks is the low-hanging fruit in shoring up an organization's security posture.

According to the PWC 2012 Information Security Breaches Survey, organizations with a security awareness program are 50 percent less likely to have staff-related security breaches than those without awareness training.[ii]

Dell SecureWorks offers a comprehensive suite of Security Awareness Training Solutions to help organizations teach their employees secure behavior and reduce risk. For example, Managed Phishing Services train employees to recognize phishing attacks and take proper action when receiving suspicious emails. Dell SecureWorks will send employees phishing emails using the same tactics attackers use. When employees click on a suspicious link or attachment, they receive immediate feedback, providing them with a "teachable moment."

"Mitigation without education causes users to repeat 'bad' behavior without understanding they are acting 'badly'," observes Elliot Lewis, the Chief Security Architect of Dell Software Group. "Active education is one of the best ways to reinforce good behavior. This should be a primary feature of any security program."

UMC Health System, the primary teaching hospital for the Texas Tech University Health Sciences Center, has implemented an aggressive education and security awareness program with demonstrable results, according to Phil Alexander, Information Security Officer at UMC. The program includes quarterly "lunch and learns" and "phishing tournaments" that demonstrate phishing techniques and teach employees about the risks, he explained in an interview at the 2014 Privacy & Security Forum in San Diego.[iii] Alexander recounted a specific example of employees—who'd been repeatedly educated on the importance of not responding to unknown or untrusted queries—reporting suspicious phone calls purportedly from a supplier, asking about the printers, faxes and copiers used on the UMC network.

"We always say that if it smells a little fishy, report it, [but] these [employees] called my office to say, 'hey, someone's calling here asking about what type of printers and faxes we have, and it just sounded odd,'" he recalled. "Normally, they would have just given that information over."

Identity and access management
Security technology and processes also play an important role in reducing the most common human errors that create vulnerabilities. Among the most familiar is failure to create strong and unique passwords for sensitive data and applications. A recent study found that approximately 76 percent of attacks on corporate networks involved weak passwords.[iv]

Identity and Access Management (IAM) goes well beyond password management and has become a strategic imperative for enterprises as they strive for greater agility. Dell One Identity solutions apply automation and shared intelligence that reduce complexity and improve ease of use. It also provides the

Forward-thinking organizations invest in more than just technology to shore up their IT defenses. They work to educate, train, and cultivate a 'culture of security' among employees.

flexibility needed to tailor a solution to an organization's unique needs.

Effective IAM helps improve business agility and secures the enterprise in these key areas:

- **Identity governance**—places control and visibility in the hands of the business, governs application access, access to data, and privileged accounts, and provisions and de-provisions using self-service and unified policy, workflows and reporting

- **Privileged management**—gives organizations the ability to ensure individual accountability for shared accounts, provides least-privileged access to administrator accounts, and logs and records all administrative activity

- **Access management**—ensures appropriate access enterprise-wide, single sign-on—all users, devices and locations—that reduces complexity and automates processes for security and compliance

That's precisely the type of control needed by the Hawaii Department of Education (HDOE), with upwards of 25,000 employees often tasked with daily access to 10 or more major applications—previously all with unique sign-ons and URLs. Asking employees to remember all that information could constitute a part-time job in itself, as well as a potential security risk. And the department's customer service desk was suffering a continual barrage of requests to reset passwords. The situation sparked frustration among teachers and administrators who sometimes lacked access for extended periods. It also redirected the IT staff's focus to lower-level tasks, many of which could be automated with well-chosen technology.

The Dell One Identity solutions HDOE deployed added true identity management with an advanced proxy service to tightly control user access. It instantly checks all access requests when employees click on a particular icon. The technology allows seamless access to the application or content when, and only when, it detects a valid session identifier and an authorized, authenticated user. It gives the department the ability to:

- Remove vulnerability of systems, data and applications

- Support a wide range of authentication methods and security systems

- Enable single sign on (SSO) across multiple web servers

- Provide access and control by a user's role

- Add compliance with audit, access control and separation of duties features

The solutions helped HDOE rein in increasing IT sprawl and provide all employee groups with easy access to resources they need, without adding infrastructure or complexity. And its 25,000 users no longer have to resort to simple, vulnerable passwords—or writing them on Post-it notes—to efficiently get their jobs done.

Mobile and endpoint security

Another key to mitigating human error is strong security at network endpoints and mobile devices that access data—particularly sensitive customer and financial information. A recent study found that theft or loss of a computer or device accounted for 27 percent of data breaches.[v]

Education and access management can't eliminate *every* lost laptop or ill-advised click on a suspicious email or website link. When they happen, multi-layered endpoint security can block dangerous spam and malware and find potential endpoint vulnerabilities, while encrypting the enterprise data residing on endpoints.

Dell Data Protection | Encryption (DDP |E) and Dell Data Protection | Protected Workspace (DDP | PW) work in concert with IAM and next-generation firewalls to protect data against many of the common human errors: lost or stolen mobile or storage devices, unauthorized use of cloud services, opening virus-infected email attachments and the like. And it does so in a more informative way and without adding administrative complexity.

A large Midwestern U.S. bank that manages nearly $17 billion in assets needed that type of protection against the four or five lost or stolen employee laptops it suffers each year. To protect sensitive operational and customer data stored on PCs, laptops and USB drives, the organization decided to encrypt data on all its devices long before this became a regulatory requirement. It needed an encryption solution that could be deployed quickly and easily, without negatively affecting employee productivity. The solution also had to provide a single management console without adding additional administrative burden; manage security on all device types; and ensure fast, full recovery of encrypted data on demand.

Deploying DDP |E helped reduce administrative burden through the single management console for multiple devices, provided a faster logon process for employees, and was able to recover lost or corrupted data in less than 20 minutes. A phased rollout with ongoing Dell support dramatically reduced deployment risk. And acting early allowed the bank to make technology decisions based on real business needs — not looming deadlines.

For customers who want a 24x7 managed security service, Dell employs its Advanced Endpoint Threat Detection Service to provide the earliest possible warning that endpoints may be hosting an advanced adversary. This fully managed service heightens security situational awareness by warning when endpoints may have been compromised and, by accessing extensive intelligence on threat actors and actor tradecraft, accelerates incident response efforts by pinpointing exactly which systems are compromised, how they were compromised, and how you can repair them.

Network security

A centerpiece of IT security remains next-generation firewalls. They help mitigate human slipups, monitoring traffic on a network and delivering intrusion prevention. But they can also play an important role in the ongoing education of end users. All this without impacting network performance – and by extension end-user productivity.

Application control at the network level mitigates the risks posed by users visiting questionable websites or running web applications by allowing IT and security teams to specify approved applications, while explicitly prohibiting other applications or whole categories of applications. But by adding in end-user training, the effectiveness of these security measures increase. After all, 64% of employees admit to visiting non-work related websites every single day.[vi]

"If users go to a website and the security simply blocks that website and doesn't tell them why, they will just find another way to get to the website," says Dell's Elliott Lewis. "Now, if the software tells users why the site is dangerous, there's a much better chance they'll do the right thing and not go there anymore."

For organizations to truly secure their information, they need employees, partners and others with access to their data to understand, embrace and comply with well-articulated security policies and protocols.

Two other key elements of network security solutions include:

- Secure remote access capabilities that extend SSL virtual private network (VPN) access to employees and extranet business partners with two-factor authentication to mission-critical resources from virtually any endpoint—including desktops, laptops, smartphones and tablets.

- Email security solutions with protection from viruses, zombies, spam, phishing that leverage multiple threat detection techniques.

This type of protection helped Massage Envy Spa reduce IT complexity at more than 960 franchised clinics by standardizing on a range of Dell hardware, software and SonicWALL firewalls. Massage Envy IT security staff increased control, reducing malware by 30 percent, and saved 20 hours each month eliminating manual processes in managing its firewalls.

"We can make a global change to all of the firewalls in just one region or standardize the firmware on firewalls at 10 clinics in just a few minutes," said Stacey Arellano, Massage Envy's IT Program Manager. "We made it possible for franchise owners to focus on running their business and not be distracted by IT issues by creating a better, more secure IT platform."

Equally important, Massage Envy engineers have been able to protect users at the clinics from themselves, blocking 55 out of 64 web-content categories that are either dangerous or unproductive.

"We can keep employees off of social media and still grant access for those who need it by using the Dell SonicWALL Content Filtering Service in our Dell SonicWALL NSA and TZ series firewalls," notes Adam Jacobi, Massage Envy's director of IT services.

People as assets, not liabilities

Technology defenses are, of course, a critical component of managing threats, but their effectiveness is limited without the processes and people that make them stick. Through sustained education and awareness that changes the behavior of the workforce, as well as automation and governance, companies can transform today's liabilities – their employees – into tomorrow's assets, developing a culture of compliance and a workforce that acts as stewards of information security.

To do this, technology, process and people must work seamlessly together. Dell facilitates this relationship by developing end-to-end IT security solutions that are easy to use, designed to be embraced by employees and business partners without hampering productivity. More adoption means more compliance, and better security. And better security *is* better business.

To learn more, visit Dell.com/Security and follow @DellSecurity on Twitter.

[i] http://www.ponemon.org/local/upload/file/Post%20Breach%20Boom%20V7.pdf | Ponemon Institute© Research Report: The Post Breach Boom, February 2013

[ii] http://www.cutimes.com/2014/04/03/your-employees-can-prevent-cyberattacks

[iii] Phil Alexander - Privacy & Security Forum 2014 San Diego, Healthcare IT News, July 24, 2014, retrieved at: http://www.healthcareitnews.com/video/phil-alexander-privacy-security-forum-2014-san-diego?mkt_tok=3RkMMJWWfF9wsRonuqrMZKXonjHpfsX84%2BkvULHr08Yy0EZ5VunJEUWy2YIIRNQ%2FcOedCQkZHblFnVUKSK2vULcNqKwP

[iv] http://www.cloudentr.com/latest-resources/industry-news/2014/3/19/weak-passwords-among-top-causes-of-data-breaches-tips-for-password-security

[v] http://resources.infosecinstitute.com/2013-data-breaches-need-know/

[vi] http://www.employeepc.com/guide/employee-productivity.htm