Data Security in a Zero-Trust Environment

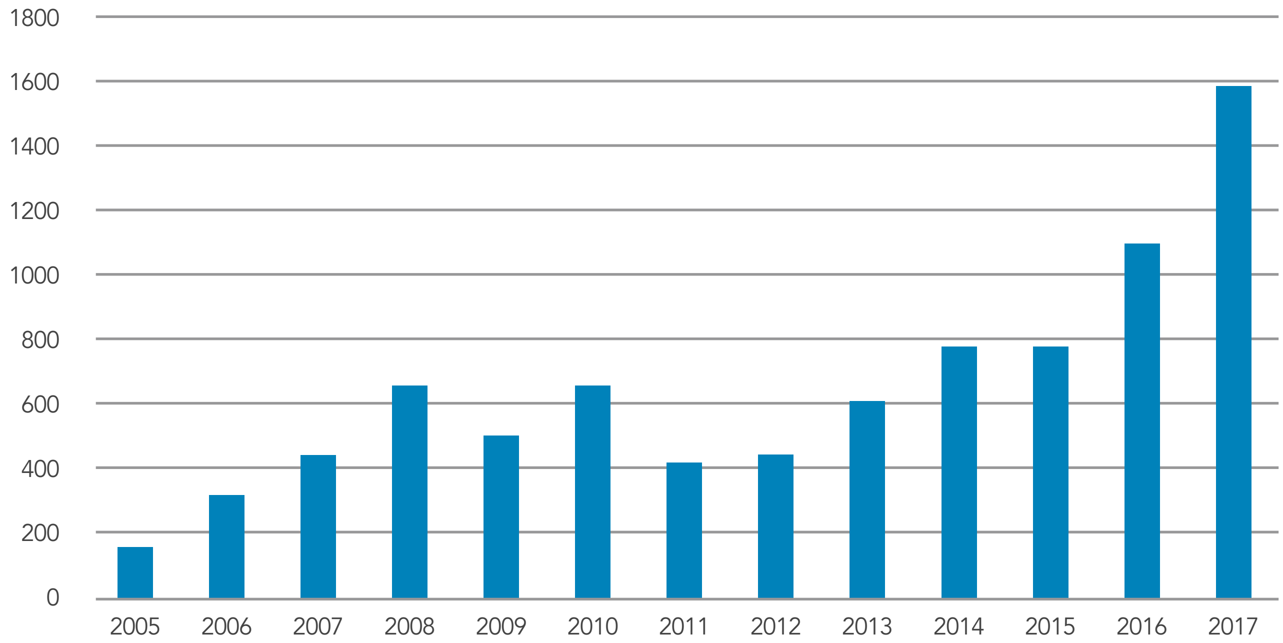
Employee data protection & the transition from HR to IT

For most companies, the Human Resources department has a long history of guarding sensitive employee data. Rows of beige file cabinets line a back closet where only those with a key and knowledge of the filing system have access to the personal information of countless employees. The greatest risk to this data has always been fire or water damage, but that's quickly changing with the emergence of online data storage.

Today, a combination of IT and your data security personnel are likely the protectors of your most sensitive information. Unfortunately now that all of this information is out of hand and off desks, it is easy to forget that data security is a team effort where all parties are responsible. Regardless of the security measures put in place by the company, careless sharing of passwords by employees or simply being unaware of potential threats can negate best efforts.

Computer Business Review estimates that some 4.5 billion records were compromised globally in the first half of 2018 alone – 41% by accidental loss or a malicious insider. Since 2005 the **Identity Theft Resource Center** has tracked an alarming rise in U.S. data breaches, with nearly 1600 major incidents reported in 2017, and not since 2011 has there been a decline in the number of annual data breaches in the U.S.

U.S. Data Breaches



Source: Identity Theft Resource Center

Who is responsible for data protection?

In July 2018, a **UnityPoint Health employee fell victim to a widespread phishing attack** exposing 1.4 million patient records. These types of attacks have become more sophisticated as criminals leverage social media to target unsuspecting employees with bogus requests. Using sites like LinkedIn, data thieves are able to identify key personnel within large companies along with those employees who report to them. They then craft phishing emails that appear legitimate and request passwords or other information which allows the hacker access to front office systems or even back end databases.

The **IBM Security: Examining the 2018 Cost of a Data Breach** report estimates that the average data breach costs companies $3.9 million and takes 69 days to contain. With this level of risk exposure, it is within every organization’s best interest to get serious about data protection.

What can you do internally?

Educate your employees. It is critical that businesses adopt a zero trust policy where employees are conditioned not to instinctively trust requests for passwords, system access, monetary transfers, or sensitive data – even from superiors or fellow colleagues. Phishing attempts are on the rise and zero trust policies safeguard both data and employees.

Adopting a strong technology use policy and requiring employees to complete annual data security training will further enhance the efforts of IT to secure company data. Instructing employees to verify a request either in person or orally before exchanging sensitive information will thwart most phishing attempts. It is also wise for IT and security groups to disseminate common or new threats to employees regularly. The United States Computer Emergency Readiness Team (US-CERT) is a real-time source for security threat information and can be found **here**.

Implement strong password policies. Employees should be vigilant in protecting their passwords and IT should adopt stringent password policies to keep employees from sharing passwords across business systems. Businesses should refrain from utilizing "commonly known" passwords and utilize single sign-on technologies where possible.

Automatic locking of devices enhances the level of protection offered by passwords and prevents both internal and external users from gaining unauthorized access via unattended or lost devices. Encouraging employees to set complex passwords and forcing regular password changes can protect from saved passwords being accessed on misplaced or shared devices.

Use the technology available. Data security is big business and companies around the world are working just as fast as the individuals looking to hack your systems. Technologies exist to help organizations secure their sensitive data. Penetration testing and applications monitoring software like **Singtel's TrustWave** exist for the sole purpose of fighting cybercrime and reducing risk.

An often overlooked technology that can be deployed without the purchase of a new tool is email flagging. Flagging external emails as "EXTERNAL" can alert employees to phishing attempts. Many companies have begun prepending statements to external emails warning employees of the untrusted source from which the email originated. This feature is standard with most email hosting services and can be configured in minutes. It's also wise to include a statement in external emails warning employees about clicking links or downloading files as these actions can install ransomware and other viruses.

How can we ensure our vendors are secure?

With the proliferation of software as a service (SaaS), thousands of software companies have emerged with promises to revolutionize business, but it is critical to understand that good security plans take expertise, time to implement, and often cost a lot of money. Third-party audits alone can run in the hundreds of thousands of dollars annually and secure data hosting with the proper security infrastructure and tools can easily double these expenses just to get started.

While industry best practices and security standards exist, it is often challenging to understand how they translate to your business. Depending on the data being secured, the standards may vary. For example, to securely store payment card information vendors should be PCI compliant, but if they are storing employees' personal data SOC 2 or ISO 27018 should be required. While overlap is common between security certifications, each has a set of controls that auditors review when auditing a company. Here are some of the common security standards that SaaS companies display.

- **ISO 27001 – Security Management Controls**
- **ISO 27017 – Cloud Specific Controls**
- **ISO 27018 – Personal Data Protection**
- **PCI – Payment Card Standards**
- **SOC 1 – Audit Controls Report**
- **SOC 2 – Security, Availability, Processing Integrity, Confidentiality and Privacy**
- **SOC 3 – General Controls**

AICPA Service Organization Control Reports
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports ®

Privacy Shield
Framework

ISO 27017
International Organization for Standardization

ISO 27018
International Organization for Standardization

In addition to security standards, it is wise when procuring cloud-hosted business software to review each vendor's privacy policy. New legislation protecting citizens' rights to data protection is changing the way organizations control personal data. In May 2018, the General Data Protection Regulations (GDPR) went into effect, instantly changing the way SaaS vendors store, share and process the personal data of European Union data subjects. Because of challenges identifying who in fact is an EU data subject, reputable SaaS vendors have extended the provisions to all of their users. To coincide with the legislation, the U.S. Department of Commerce enacted Privacy Shield, creating a means for U.S. companies to become certified to host EU data in U.S. data centers. Industry insiders widely expect that the United States and individual states will adopt data protection regulations in alignment with GDPR in the coming years. It is wise for businesses investing in new technology products that store personal data to ensure potential vendors meets these qualifications now, or risk losing that investment as legislation is enacted to protect domestic users. To check if your vendor is Privacy Shield certified, search **here**.

Businesses should also ensure their vendors are utilizing industry-leading data centers for hosting sensitive data. These providers include Amazon Web Services (AWS), Microsoft Azure, Rackspace, and Google. Securing data is expensive and doing it well requires economy of scale. AWS hosts more than 1 million enterprise customers in 190 countries and hundreds of shared data centers, providing it with the resources to secure the data of customers large and small. AWS also holds all of the security standard certifications listed in this article, as do Microsoft Azure and Google.

What if we are breached?

With data breaches continuing to rise, regardless of the chosen SaaS vendor or cloud hosting provider, organizations should be prepared for an incident at any time. Be sure to request proof of cyber insurance in excess of $5 million per occurrence from potential vendors. With the average cost of a data breach exceeding $3.9 million in 2018, coverage under a vendor's cyber insurance policy could save the business.

Cyber insurance often includes third-party breach investigation, legal counsel, and breach notification as well. All of these pre-arranged services are important during an incident - when time matters most. Many state laws require timely notification for breach victims, and without proper services in place to investigate a breach, contain the breach, define the legal requirements, and properly notify the victims, organizations risk compounding their loss of money and reputation – and possibly risk criminal action for negligence.

Ultimately it's everyone's responsibility to protect sensitive data. The common password is the new HR key and all employees, vendors, and third-party service providers should be doing their part to ensure the security of people's sensitive data. By training the employees, vetting the vendors and third-party service providers, and preparing for the worst, business leaders can rest easier knowing their data is in the best possible hands. Potential vendors meets these qualifications now, or risk losing that investment as legislation is enacted to protect domestic users. To check if your vendor is Privacy Shield certified, search here.

How TCP can help

TCP is an industry leading time and attendance solution provider. In time and attendance, accuracy is everything. Anything less can result in problems with payroll, upset employees, ruined credibility with HR and the C-suite, and even wage-and-labor noncompliance penalties. Accurate time and attendance demands technology that ensures compliance and captures every process, rule, and exception. It also requires flexibility and personalization to account for your unique needs. For this, you need a partner dedicated to protecting the sensitize data of your people and with a shared desire to make your entire payroll system work flawlessly. Since 1988, TCP has been on a mission to take care of people — not businesses, not time clocks, not even payroll. People. We go above and beyond because we want to protect our people, our customers, and anyone who's impacted by our business. Today, TCP offers a comprehensive workforce management system that helps thousands of organizations optimize operations and streamline processes.

TCP's TimeClock Plus software is offered as a SaaS solution, hosted in the AWS cloud. These solutions are available to customers through purpose-built web applications, application programming interfaces (APIs), hardware terminals, and mobile applications.

TCP's primary security focus is to safeguard our customers' and users' data. This is the reason we have invested in the appropriate resources, controls, and independent oversite to protect and service our customers around the world. This investment includes the implementation of a dedicated Security Team and Data Protection Officer (DPO). The Security Team and DPO are responsible for TCP's comprehensive security and risk management program and the governance process. The Security Team is focused on defining new and refining existing controls in accordance with industry best practices, implementing and managing the TCP security framework, maintaining legal compliance for our business and our customers, as well as providing a support structure to facilitate effective risk management.

Additionally, we've built our platform atop an industry-leading cloud provider, Amazon Web Services. TCP is SOC 2 Type II and SOC 3 certified, GDPR complaint, and U.S. Privacy Shield certified. Our AWS data centers hold NIST certifications, SOC 1, 2, and 3 certifications, and ISO 9001, 27001, 27017, and 27018 certifications. Both our products and hosting environments are routinely tested and monitored, download our SOC 3, **Global Data Privacy Policy**, and full **Security Overview** to read more.

Want to learn more about TCP? Let's talk.

866.783.9890 | www.tcpsoftware.com | **Your Workforce Ally**