DIGITAL FORTRESS

Cyber security, like customer service, is everyone's job.

BY IAN T. RAMSEY, SARAH C. SPURLOCK AND ADAM M. SMITH

THE U.S. DEPARTMENT of Homeland Security's motto regarding cyber security is: "Stop. Think. Connect."

Unfortunately, the first two directives are often ignored. Data breaches exist because we have not stopped to think and discuss data security before getting online. We are so used to just plugging something in and expecting it to work that we don't consider the consequences when technology fails us.

The construction industry was an early adopter of mobile technology, first by using mobile telephones and eventually wireless computer systems to connect personnel at remote job sites. That same practical approach continues today, with projects being managed and designed via handheld tablets and powerful computer servers that can handle everything from 3D building software to fully integrated on-line construction build and draw schedules. All of this technology is aimed towards the single purpose of safely constructing what was promised, on time and within budget.

> A data security plan is just a piece of paper unless you have the right team to update, practice and implement the plan when a breach occurs.

While technology has made the construction process more efficient, it has not changed the fact that it is people who are doing the work. That is why, for example, a computer doesn't lead the morning job-site safety meeting. And the same is true for data security meetings. Who is making sure that if technology fails, a project can still be delivered as promised, on time and within budget? Cyber security involves humans anticipating issues that technology won't always catch—especially if it's been disabled or compromised.

Everyone is Vulnerable

Understand where you are vulnerable. Data security is much more than computer software. A breach can occur with a simple, unintended disclosure like when you send an email to the wrong person. A breach can happen when a device is lost or stolen. Your company could be hacked or, more likely, an employee could (unwittingly or otherwise) introduce malware or a virus into your systems. Your data can also be intercepted by unauthorized users because of non-secure transmissions, obsolete devices or outdated or imperfect software. General contractors may need to coordinate access to confidential data with owners, subcontractors, design professionals or others, and these third parties are equally responsible for your data security. Subcontractor and vendor security failures occur often. The Target data breach was linked to an HVAC vendor, for example. Finally, employee theft is on the rise because of the ease in which large amounts of data can be transferred when no safeguards are in place.

Ian T. Ramsey is co-chair of the Privacy and Data Security Group, and **Sarah C. Spurlock** is a member of the Health Care Service Group and co-chair of the Privacy and Data Security Group, both in Stites & Harbison's Louisville office. **Adam M. Smith** is an attorney and a member of the Construction Service Group in Stites & Harbison's Lexington, Ky., office.

All of this might seem overwhelming, but it doesn't have to be. Think about data security just like the morning safety meetings. Make it top-of-mind so it becomes a part of the daily practice. The most significant threat to data security is, frankly, your employees because they have too little working knowledge. Empowering them to make their online experiences safer will pay dividends for your company's data security strategy. A change only happens if they learn and retain information. This means day-long training and large manuals do not have the focus to be effective. Start small with an easy-to-understand concept that carries into their personal life.

The Power of Passwords

Our advice is to start with passwords. Don't allow your employees to use the same password or variations that they use for their personal accounts. Anything having their name, identifying a child, home address, a pet's name or information that is easily learned from social media accounts should be barred. For mobile devices, demand that a minimum of six characters be used and require that automatic inactive locking be enabled. For laptops or desktops, use a passphrase akin to a complete sentence. The trick is to think of a quote from a movie or a line from a song, or pick random sentences from a book.

Whether to change passwords on a regular basis is a topic for debate. Password expiration policies have become the norm, so many industries follow a 60- or 90-day requirement. However, that does not mean that your company needs to follow this line of thinking, as there are many reasons why creating and keeping strong passwords is a better security practice. If your employees follow the above suggestions by creating a passphrase of 12 characters or longer and using a combination of uppercase, lowercase, numbers and symbols, then having a password expiration policy requiring scheduled changes is less critical. You will, however, need to still have a policy listing those events where a password change is required due to a data breach or malware.

Of course, even some of your best employees might not adhere to a policy of strong passwords. And in cases like this, regular password changes might keep your company ahead of the breadcrumb trail of poor passwords some employees are leaving behind for hackers to find their way into your company. The other benefit of a regular password change is that the employee gives at least some thought to data security on a regular basis—and perhaps gives your data security personnel a reason to visit with employees to discuss data security.

Don't Take the Bait

In addition to passwords, educate your employees on topics like phishing (fraudulent emails sent under the guise of being from reputable sources in order to obtain sensitive information). Hackers increasingly use these emails to get into company servers or as the first step towards a more sophisticated intrusion. A recent trend includes encryption malware that holds data hostage until a ransom is paid. The ploy might seem obvious, but the Pentagon data breach occurred when a single employee opened a malware infected email.

Therefore, training your employees on how to recognize and avoid the bait is a simple yet important piece of your overall data security plan. Here are some tips to share with your employees on how to spot a problem email:

- **Validate the sender** by verifying the sender's email address
- **Don't be fooled by graphics**, which are often stolen from legitimate websites
- **Be suspicious and check all links and attachments** by hovering your cursor over the link
- **Watch out for threats and warnings**, which is a common trick to scare you into quick action
- **Misspelled words and poor grammar** often signal a scam or malware
- **Don't let personal information or details fool you** because a motivated hacker will take the time to collect this information
- **When in doubt, make a telephone call to the IT department!**

Big Picture

Data security involves the big picture too. Consider these suggestions to evaluate where your organization stacks up.

Know Your Data. Identify, protect and limit access to your most secure information, which should include all customer and employee personally identifiable information. Consider compartmentalization by keeping the most sensitive information on separate encrypted servers. Being transparent is important; however, distinguish those who really need access from those who merely want it.

Know Your Plan. A data security plan is just a piece of paper unless you have the right team to update, practice and implement the plan when a breach occurs. An employee's title might be important to the chain of command, but the ability to solve problems calmly and quickly under pressure is paramount.

Data Security Minimums. Designate an employee to maintain a security program. Anticipate and limit risk via employee training, detection and prevention of system failures, imposing disciplinary measures for violations, preventing access by terminated employees, contractually requiring subcontractors and service providers to maintain security, limiting and controlling physical access, monitoring and reviewing effectiveness and documenting all responses to incidents.

The days of leaving data security solely in the hands of those with technical expertise are over. Take steps now to position yourself and your employees as the front line of your organization's defense against a data breach. ■