Security: A Shared Responsibility between Marketing, IT and Attorneys

by Deb Dobson of Fisher Phillips LLP, Jeff Hirner of One North, and Erin Illman of Bradley

As Marketing teams' investment in technology and use of data-driven strategies continues to rise, so should their concern over keeping that information secure. These days, the responsibility to do so no longer lies solely with the firm's IT department. Every department, and really every employee, should work together to ensure that a culture of security permeates the firm. The marketing technologist has an additional responsibility – to protect the law firm's brand.

What's the best way to do that? The truth is, there are many moving parts and, when done right, it's an ongoing effort. However, if you keep the following six things in mind, you'll establish the right guidelines to ensure your people, processes, and technologies remain secure.

1. Designate an owner and build a team.

Because everyone ultimately plays a part in keeping your firm secure, it can be difficult to determine who will keep track of the initiative and its progress. What you don't want to happen is for everyone to think someone else is handling it – because things just won't get done, putting the firm at risk. Instead, we recommend designating someone to be responsible for corralling the appropriate groups, setting and documenting the strategy, and reporting progress back to the team.

It's important to note that this does not mean it's this person's job alone to ensure the firm keeps security and privacy best practices in mind. What it does mean is that the firm will have someone to drive the initiative and hold everyone accountable for playing their part. Once everyone is aware of and agrees on who will own the process, you can carry out the other important tasks.

The Why's and How's of a Cyber Attack

According to the **2017 Official Annual Cybercrime Report**, "cybercrime damages will cost the world $6 trillion annually by 2021." In an attempt to combat this, Gartner predicts that worldwide enterprise **security spending will grow eight percent** in the next year alone, reaching more than $96 billion. In addition, the **Ponemon Institute** has concluded that the three occurrences that have the greatest impact on brand reputation are: environmental disasters, poor customer service, and data breaches.

These startling numbers have ignited many firms to take action by building an army of innately suspicious employees, all of whom feel empowered to combat any suspicious requests or traffic that comes their way. But how do you educate your people to know what to look out for? What's behind the actions of a malicious hacker? And what methods are they utilizing to tap into your most vulnerable entry points?

CONTINUES ON NEXT PAGE

A key element to success in the realm of information security is building a cross-functional team, led by the designated owner, which can support the marketing team's efforts. For example, there needs to be a legal and compliance liaison, an IT liaison, and an HR liaison. All of these players need to work together to identify issues, thoroughly review the legal and compliance obligations of the organization, effectively address decision points, and then operationalize those decisions in the organization's technology structure and among its employees.

2. Audit your current data and technologies.

Keeping an inventory of the different types of data you are currently storing/processing and the technologies you are using will help you develop the right processes to keep them secure. Once you know what data is included in your ecosystem, classify it. Is it internal data, confidential data, personal data, or public data? Under some international laws, you may need to not only know what data you collect and store, but you may also need to analyze your legal basis for processing that data. In other words, your firm will need to undergo a data audit to determine what data points you collect, store, and process, and you will also need to understand all of the uses of the information, ensuring the use is a legal basis under the relevant law that applies.

A critical component of any data-driven strategy is to first understand whose data you process, and then determine what laws and regulations apply to that processing. It is imperative to understand what kinds of marketing activities are allowed, and in what circumstances.

Once you've labeled and analyzed the legal basis for the processing of the data, decide who should have access to it – remember to limit access to those who absolutely need it, and no more than that. Finally, establish an onboarding/offboarding process to ensure access remains tightly managed.

From a technology perspective, knowing which technologies you're using will help you keep up-to-date on any critical patches or updates you should install to keep them secure. At some point, you may have to retire current technologies for security reasons. Maybe the developer of that technology isn't keeping up with security best practices, or maybe it plans to sunset support of the tool in the near future. Performing regular audits will help you plan ahead for these situations.

Having a dedicated team, or external vendor, that performs full security assessments for your current technologies can help with this process. Be sure to keep this team informed when you want to add new technologies as well. They can do a pre-assessment and help you decide if the new or emerging technology you'd like to give a try aligns with your firm's security standards. If it does, they'll know to add it to their inventory list for the next audit.

3. Establish a security budget.

This one goes hand-in-hand with the previous point. Technology changes much faster than we can keep up. Reserving a contingency fund for unexpected changes will help you stay on top of critical updates. For example, many browsers began rolling out upgrades last year that introduced a warning to users if they visited websites that didn't have an SSL certificate. The warnings labeled these

Typically, hackers are driven by one of the following motives:

Defacing the Brand:
Hackers sometimes carry out an attack in an attempt to harm or leverage your brand. Often predicated by political agenda, in this situation the goal is to paint your firm in a bad light, misrepresent what you stand for, publicly shame you for an action you have taken, or capitalize on the popularity of or traffic to your site. Vigilante hacking groups such as **Anonymous** are known for carrying out these kinds of attacks. If your attorneys are working on sensitive matters or representing controversial subjects, your firm has the potential to fall victim to this group's mission.

Accessing Sensitive Data:
A normal, clear-headed individual wouldn't part with his or her login credentials, financial information or social security number willingly. Hackers have grown more creative and sophisticated in their attempts to gain access to this information. Whether it's feeding their bank accounts, stealing

CONTINUES ON NEXT PAGE

sites as "not secure," even if they were legitimate companies. Most firms understood the importance of purchasing an SSL certificate to reassure visitors, but many had not budgeted for this additional expense. Setting aside money for changes like this, or other security or privacy vulnerabilities that are uncovered (think software bugs or new regulation like GDPR), will ensure your team can jump right into action to address them.

4. Educate your employees.

You can't expect your people to join the effort to keep your firm and your clients secure if they don't know what to look out for. Typically, threats don't target those they think will be difficult to bypass. Instead, they try to gain entry through the everyday employee. A careless or negligent employee who exposes sensitive information or falls victim to phishing attacks are most often the cause of a data breach. Educating your employees on the tactics hackers use to infiltrate your systems or data will help them keep their guard up (see sidebar).

Hold quarterly drills or tests whereby you create a fake hacking scenario and see how your employees react. Do they take the bait? Do they flag the suspicious behavior to the appropriate team? Once you conclude the test, follow up with additional training for those who failed your drill, and use these as examples in your next firm-wide security training, which should be held annually.

5. Hold your third parties accountable.

Think about it. Your clients and prospects hold you to a certain standard when it comes to security and privacy controls. Why should you not do the same for your vendors? In your quest to align yourself with partners that also foster a culture of security, it is important to review your contracts and conduct due diligence on your vendors. Consider also adding language to your RFPs to ensure you're only engaging with those who take security as seriously as you do. You should ask or consider:

- » What data is at issue? Does it include personal, confidential or sensitive information?
- » Are the data ownership rights spelled out and well understood? Who has access to the data and how can it be used?
    - » *Understand data flows, who will have access to it, and where it will be stored.*
    - » *Consider whether they have adequate systems in place to limit unnecessary access or vulnerability.*
- » Does the transfer of data comply with all applicable laws? Is the data stored beyond U.S. borders, or are there employees and subcontractors outside the U.S. who will have access to the data?
- » Use pre-qualification reviews, audits and certifications.
    - » *Are your vendors GDPR and SOX compliant? Certifications such as ISO 27001 are also good indicators of a potential partner's security capabilities.*

identities, or uncovering confidential information, the ultimate goal here is to dupe the user into sharing information they otherwise wouldn't.

Demanding Ransom:
Once armed with the sensitive information or access, hackers often like to use it as leverage for something bigger. In an example that hits very close to home, hackers successfully executed a ransomware attack on a large global law firm last summer, preventing the firm from accessing its data and crippling work and revenue for weeks – a firm's worst fear.

Blocking Legitimate Traffic:
Hackers aren't always trying to gain access to something you wouldn't want them to have. Sometimes blocking a firm's access to its clients, prospects, people, or other legitimate traffic can be just as damaging (or even more). In the fall of 2016, hackers infamously targeted Dyn, a cloud-based DNS provider with many high-profile clients – including Netflix, Spotify, and Twitter – crashing thousands of sites that used the company to manage their domain name system.

CONTINUES ON NEXT PAGE

» Do your contracts have built-in recourse in the event of a security incident through carefully drafted indemnity rights and carve-outs from limitation of liability?

» Does the service provider have appropriate cyber-liability insurance, and what are the limits on such coverage?

» Is the service provider required to assist in transferring data back to you in the event the service agreement terminates?

» Is there a retention and disposal clause?

» Consider requiring the third party to not only indemnify you, but also cooperate with any pending litigation or investigation.

If you find that your vendors don't have the same security rigor that you do, we suggest you part ways. Risking a breach, and your reputation, isn't worth holding onto unsecure third-parties.

6. Rinse and Repeat.

As mentioned before, security is an ongoing process. The effort is never done, and the goal is always to continue improving. Revisit your audits, access, and processes regularly, and make changes as necessary. It also doesn't hurt to bring in a neutral party to help you uncover vulnerabilities you're not objective or savvy enough to uncover. Finally, develop an incident response and recovery strategy so that you're prepared in the case a data breach does actually occur. It's important that everyone understands and is comfortable with their role in the strategy. To help with this, practice executing a handful of mock scenarios throughout the year. You can't always prevent an attack from occurring, but you can prepare everyone at your firm to react in an optimal and timely fashion, reducing the collateral damage and expediting a resolution.

With cyber risks ever evolving, security must be a shared effort and tackled through a comprehensive strategy that lives, breathes and improves over time. As your firm's digital footprint grows (and it should), think about how you'll continue to keep security top-of-mind for everyone at your firm. **ILTA**

ERIN ILLMAN
As a partner at Bradley, Erin Illman co-chairs the firm's Cybersecurity and Privacy Practice Group. Erin is designated as an ANSI Certified Information Privacy Professional (CIPP/US) by the International Association of Privacy Professionals and serves on the North Carolina Bar Association's Privacy and Security Committee. She regularly advises clients on GLBA, HIPAA, COPPA, CAN-SPAM, FCRA, security breach notification laws, and other U.S. state and federal privacy and data security requirements, and global data protection laws, as well as privacy-related enforcement actions and litigation. Her practice includes representing companies in reactive incident response situations and counseling clients on a variety of e-commerce, electronic marketing, digital contracts and security issues. Erin received her J.D. from the University of Alabama School of Law and her B.A. from the University of North Carolina at Chapel Hill. Erin can be reached at eillman@bradley.com.