PLF *in*BRIEF

ISSUE 132 | AUGUST 2017

Malpractice Prevention Education for Oregon Lawyers

Anatomy of a Cyber Claim

By Emilee S. Preble, in collaboration with the Beazley Breach Response team

From headline news to state bar bulletins, ABA articles to lawyer blogs and other social media – it is hard to be a lawyer in 2017 and not know that cyber security risks are on the collective minds of lawyers and law firms across the country. In many ways, this makes sense. Lawyers are the guardians of vast quantities of confidential client information, which makes law firms a natural target for cyber criminals.

In 2016, the networks of Cravath Swaine & Moore LLP, Weil Gotshal & Manges LLP, and other major law firms were besieged by a hacking event that sought to find and leverage confidential or insider information related to large

public companies. That event made national news – covered by the *Wall Street Journal*, *Bloomberg News*, and others – and served as a confirmation for what too many in the legal community have known for years – law firms have become an attractive target for hackers. This is as true for large national firms with hundreds of lawyers as it is for Oregon solo practitioners.

As the mandatory malpractice coverage provider in Oregon, the PLF was well positioned to see the potential risk to Oregon lawyers for these types of claims increase over time. Beginning in 2013, all PLF Excess Coverage was issued to law firms with an endorsement that covered cyber liability and breach response.[1] This endorsement is serviced by Beazley Breach Response (BBR) Services. Beazley is a longtime reinsurer of the PLF Excess Program and was among the first reinsurers in the world to develop and write cyber insurance policies for businesses. Cyber claims often require the involvement of many specialized resources, including computer forensic experts, privacy lawyers, credit monitoring services, and call centers. Because cyber claims are altogether different from typical malpractice claims, the PLF's partnership with Beazley is key, as BBR has the resources and expertise to handle the complexities of cyber claims.

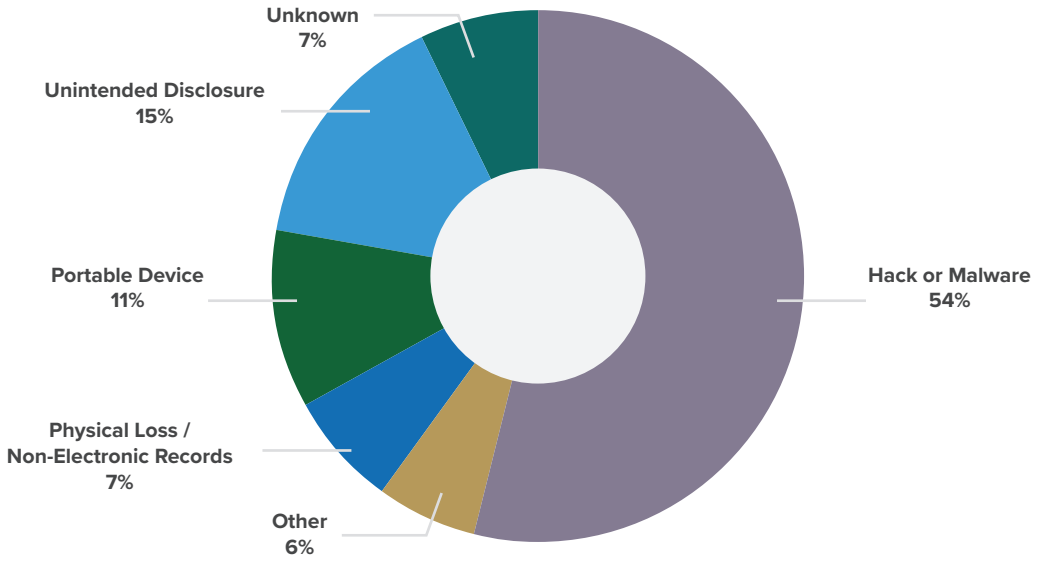
What risks do law firms face?

Client confidentiality has always been a hallmark of legal professional ethics, but protecting that confidentiality is now much more challenging and complex as the sands of technology shift over time. In this brave new world of both ever-changing technology and constantly evolving cyber threats, lawyers need to know how to best safeguard their data. Though some firms have the benefit of in-house IT staff to safeguard their systems, many law firms, particularly small and solo firms, may not be able to devote adequate resources and time to information security. In addition, not all cyber attacks are the result of inadequate technology protections. Lawyers and staff must be trained on how to prevent the hackers from entering the system. One click on a hacker's seemingly innocuous link or email attachment can result in an attack on the firm's entire network.

The chart below shows how U.S. law firms covered by Beazley experienced cyber attacks in 2015 to 2016.

2015–16 Law Firm Incidents[2]

Reprinted with permission from "BBR Industry Insights – Law Firms"



[1] The PLF Primary Plan excludes these claims in Section VI.20 – Confidential or Private Information/Computer Systems.
[2] Data from U.S. claims reported under BBR Services coverage.

"Everything went very smoothly. They [BBR Services] were responsive and helpful in making sure we complied with all the best practices standards. I was able to get everything wrapped up in just under two weeks. It was good to have a prompt response team in place for something time sensitive. I also appreciate how Beazley handled everything professionally and politely. It all helped keep the situation manageable for me and enabled me to get back to work with only a minimal loss of productivity."

–PLF Excess-covered lawyer with a stolen laptop in 2016

What's happening in Oregon?

Since the PLF Excess Program began offering cyber coverage in 2013, eight claims were reported to and serviced by BBR.

2017	2016	2015	2014	2013
3 claims *(as of July 13, 2017)*	4 claims	1 claim	0 claims	0 claims

Of those eight claims, seven involved some kind of theft (vehicle or office break-in, stolen laptop/tablet, stolen briefcase). This pattern differs from the national law firm trend. Looking at the chart on page 4, 15% of all cyber claims BBR serviced dealt with Unintended Disclosure (including stolen property), whereas for the PLF program, that type of claim happened 87.5% of the time.[3] The tendency in Oregon reported claims resulting from theft should be read cautiously, as the sample size and timeline is very short. These types of claims are also likely reported more often than other types of cyber claims as the loss is known immediately. All that said, it is interesting to note these early trends in cyber claims for firms covered under PLF Excess.

What can you do to protect your firm?

This is a question we get asked a lot at the PLF. The first step would be to make sure your law firm is covered by a cyber insurance policy. The mandatory PLF Primary Coverage specifically excludes these types of claims (2017 PLF Primary Plan, Section VI.20). Cyber coverage is available on the commercial market and can be included as an add-on to most excess coverage. PLF Excess Coverage automatically includes a cyber endorsement for firms with limits of $100,000 for firms of 1–9 lawyers, and $250,000 for firms of 10 or more lawyers. Limits above that are available on a separately underwritten basis.

A high percentage of Oregon cyber claims result from theft or physical loss of devices. So the next step would be to take measures to protect your devices and the data stored on them. Never leave your portable devices in a vehicle. (Even trunks are unsafe because they can be accessed via fold-down seats.) Offices can also be unsafe, as they can be burglarized. While you may never be able to guarantee the physical security of your devices around the clock, you can take some important steps to secure the data on those devices. Using encryption and a strong password can help reduce the likelihood a hacker will gain access to your client data, even if the device is stolen or compromised.

[3] The other lone claim involved a possible network breach at a third-party provider, but notices were required.

In addition to ensuring your firm has coverage for these events, it is also important to make sure your firm takes appropriate steps to reduce the risk of data loss. Our partners at BBR have provided the following list of steps law firms can take to reduce the risk of cyberattacks.

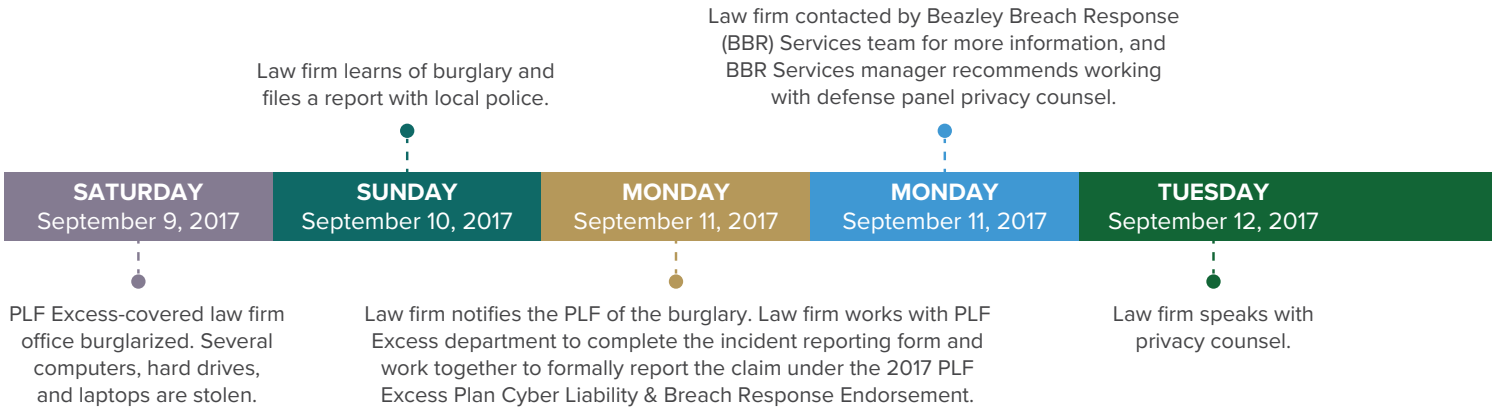
Cyberattacks against law firms are on the rise, and they are happening here in Oregon. Educate yourself about the potential risks and take the steps to protect your firm and your client information. Preparation is key. ■

- **Incident response planning.** Develop an incident response plan, designate your incident response team, and practice and update your plan regularly.
- **Employee training.** Train employees on security awareness throughout the year; consider phishing tests to maintain employee vigilance.
- **Risk analysis.** Conduct a risk analysis to identify what sensitive data the firm holds and where, and to evaluate your risks and the effectiveness of mitigating controls. Consider employing an experienced third-party vendor to conduct the risk assessment.
- **Encryption.** Implement full device encryption on all portable devices and consider secure email solutions.
- **Two-factor authentication.** Set up two-factor authentication for remote access and for administrator access to key resources. Provide remote access only through secure channels, such as a well-configured virtual private network (VPN) connection. Require strong passwords.
- **Backups.** Implement a data backup and recovery plan; maintain copies of sensitive or proprietary data in a separate and secure location not readily accessible from local networks.
- **Document retention policy.** Develop a document retention policy and properly dispose of sensitive data accordingly.
- **Penetration testing.** Retain a security firm to evaluate the risk that an attacker can compromise your IT assets and remediate accordingly.
- **Antivirus and patching.** Regularly update antivirus definitions for all users and ensure timely patching of operating systems and software.
- **Intrusion prevention and detection.** Deploy an intrusion detection system (IDS) and an intrusion prevention system (IPS) that aggregate logs to a Security Information and Event Management (SIEM) tool that sends real-time alerts.
- **Vendor risk management.** Ensure vendors are contractually obligated to protect sensitive data, provide timely notice of a breach, return or destroy data at termination, and maintain cyber liability insurance.

Reprinted with permission from "BBR Industry Insights - Law Firms"

Timeline of a Cyber Claim from Stolen Devices

Timeline developed in partnership with the BBR Claims Team



CLAIMS EXAMPLE FROM ANOTHER BEAZLEY BREACH

Example: Hook, Line, and Hacker

A real estate attorney fell for a phishing email and gave up his credentials. After clients started complaining about spam emails they were receiving from him, the attorney realized his email had been compromised and contacted BBR Services. BBR Services quickly connected him with privacy data breach counsel and a forensic firm. Unfortunately, the forensic firm could not rule out the possibility of unauthorized access to the attorney's email inbox, which contained client information dating back to 1990, but was able to use data mining to determine the affected population (thousands of clients). Counsel reviewed applicable state breach notification statutes and drafted notification letters and a call center script. BBR Services coordinated notification and call center services. Affected individuals whose Social Security numbers had been exposed were offered credit monitoring.

Reprinted with permission from Beazley Group

To find additional resources on information security, visit the PLF website (*www.osbplf.org*). Our practice aids include guidance on file retention, using online data storage providers, and how to back up your computer, as well as an information security checklist for small businesses. See also our *inPractice* blog (*www.osbplf.org/inpractice/*). Posts discuss two-factor authentication, encryption, and passphrases.

Emilee Preble is the lead underwriter for the PLF Excess Program.