PLF *in*BRIEF

ISSUE 140 | MAY 2020

Malpractice Prevention Education for Oregon Lawyers

LAW PRACTICE

Excess Corner: COVID-19 & Cyber Risk

By Emilee Preble, Staff Attorney / Excess Program Administrator

The dramatic shift to work-from-home setups in recent weeks has opened up the potential for increased cyber crime. Criminals may seek to exploit vulnerable home networks by deploying targeted social engineering or spear-phishing scams.

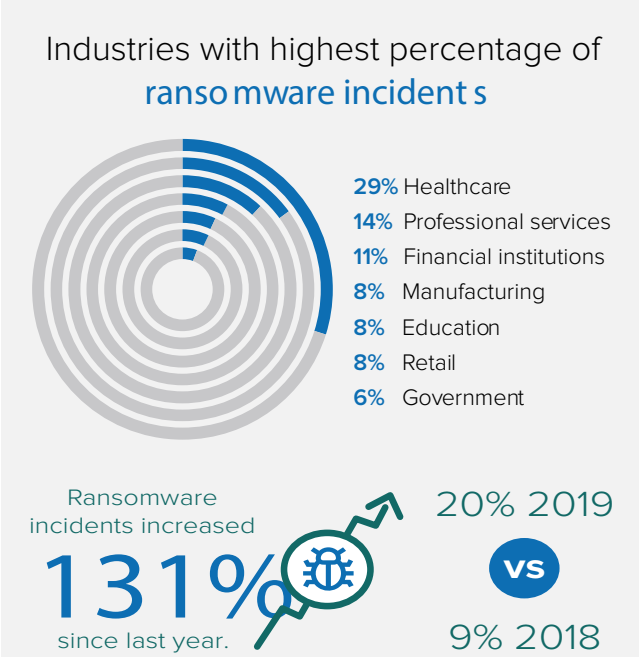
One potential cyber risk to be aware of as you work remotely are pandemic-related email scams. Be sure to regard COVID-19 related emails, particularly those with attachments and links, with extra scrutiny. It is important to confirm that these emails are coming from a known sender before opening. Cyber criminals can use our concern about the pandemic to infect home networks or computers with malicious malware or ransomware.

While claims related to the types of cyber liability described above are excluded under the PLF Primary Plan (Exclusion 20), there is coverage for these claims under a special endorsement to the PLF Excess Coverage Plan. If your firm does not have PLF Excess Coverage, you may want to review other insurance policies to see if you have coverage for cyber liability.

Firms with PLF Excess Coverage benefit from a Cyber Liability & Breach Response endorsement serviced by Beazley.* Beazley just released its 2020 Breach Briefing in which the focus was on ransomware. From 2018 to 2019, claims Beazley serviced saw a 131% increase in ransomware attacks. Included here are some excerpts from that 2020 Breach Briefing that shine a light specifically on ransomware.

If your firm is interested in Excess Coverage, please visit *www.osbplf.org > Excess Coverage* to learn more about how to apply.

**Claims handling and breach response services are provided by Beazley USA Services, a member of Beazley Group. Beazley USA Services does not underwrite coverage for the PLF Excess Program. Excess coverage purchased through the PLF is subject to the PLF Excess Program's underwriting processes.*



Content provided by Beazley, www.beazley.com.

WHO IS THE TARGET?

Ransomware can be devastating to an individual or an organization. Traditionally, these attacks were designed to deny access and interrupt business operations. However, the recent shift towards ransomware paired with banking trojans, and towards threats to expose data, changes the landscape. Anyone with important data stored on their computer or network is a target – from municipalities or hospitals through to law firms. Important data at risk was traditionally thought to be personally identifiable information (PII) and protected health information (PHI), but it could also include intellectual property, litigation strategies, unpublished financials, and project bids. It is a myth that attackers are not interested in small companies. As our data shows, small and medium-sized businesses are often easier to exploit, and therefore, very attractive targets.

WHAT IS THE ATTACK?

One common form of attack used to deploy ransomware are phishing emails. Here we explain this attack vector and ways to mitigate the associated risks.

PHISHING

Today, direct email of malware and links to credential-stealing sites lead to a large number of incidents. There are a lot of protections available, in the forms of email filters and added layers of authentication; however, few of these solutions are broadly implemented. People have access to the information and technology that the attackers want, and attackers will continue to find new ways to reach people and exploit them. It would be incorrect to view phishing as the vulnerability; phishing just happens to be the most effective way of getting to the real vulnerability – people.

MITIGATING PHISHING RISK

- Enable multi-factor authentication (MFA)
- Force regularly scheduled password resets, preventing recycled passwords
- Train employees to recognize and report suspicious email traffic

Content provided by Beazley, *www.beazley.com*.

Emilee Preble is a Staff Attorney / Excess Program Administrator at the PLF