How General Counsel Can Prepare for a Cyber Breach

General Counsel address myriad legal and business challenges, but none may be as harrowing as dealing with a cyber attack. They don’t know when a successful attack may occur, there are no guaranteed methods of prevention and incident response and impact mitigation are complex processes.

The Costs of a Breach are Significant

- Average time an attacker remains inside a network before being discovered: 78 days
- Global average cost of a data breach: $3.86 million
- Likelihood of a second breach: 27.9%

How to Prepare for the Inevitable

CONNECT
Develop relationships with leaders throughout the company. In particular, partner with the CISO to understand the organization’s data, what is important, how it is protected, where it is located and from where it can be accessed, and how much visibility the security team has into it.

PLAN
Develop an IR plan and identify the team needed to execute that plan. The response team may include the CEO, CISO, CMO, internal and external legal counsel, communications professionals (such as public and investor relations) and external incident responders and forensic specialists.

PROTECT
Establish and protect attorney-client privilege immediately after a breach (and before, if possible) by coordinating communications and incident response through the GC’s office. Given that litigation, investigations and government inquiries often follow a breach, it is valuable to have a three-way master service agreement (MSA) in place with external counsel, IR consultants and others.

INOLVE
Provide the Board (or a Board committee) with regular updates from the CISO. Fiduciary duties related to cyber security require Boards to be aware, educated and involved, and to meet a “reasonableness” standard akin to the business judgement rule.

CONSIDER
Think about getting cyber insurance within the context of the company’s overall insurance program. Knowing the costs of a breach and evaluating the risk of a loss to the company may warrant the use of cyber insurance.

FireEye is trusted by:
• 40% of Forbes Global 2000
• 6,300 customers worldwide
• 1,000 Government Agencies worldwide

Learn more at: www.FireEye.com

Businesses in nearly every industry or market experienced a breach last year.

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>23%</td>
</tr>
<tr>
<td>Government</td>
<td>23%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>5%</td>
</tr>
<tr>
<td>Retail and Hospitality</td>
<td>12%</td>
</tr>
<tr>
<td>Transportation and Logistics</td>
<td>8%</td>
</tr>
<tr>
<td>Construction and Engineering</td>
<td>4%</td>
</tr>
<tr>
<td>Education</td>
<td>4%</td>
</tr>
<tr>
<td>Entertainment and Media</td>
<td>5%</td>
</tr>
<tr>
<td>Business and Professional Services</td>
<td>17%</td>
</tr>
<tr>
<td>Energy and Utilities</td>
<td>4%</td>
</tr>
<tr>
<td>High Tech and Telecom</td>
<td>12%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
</tbody>
</table>

The good news is that several indictments were announced for major threat actors in 2018.

March: Islamic Revolutionary Guard Corps
In an indictment, the U.S. Department of Justice and Treasury accused Iran of stealing intellectual property from more than 300 universities, as well as government agencies and financial services companies.1

July: Russian Intelligence Officers
The U.S. Department of Justice announced the indictments of 12 Russian intelligence officers for carrying out large-scale cyber operations against the Democratic Party in advance of the 2016 Presidential election. The officers’ alleged crimes included the theft and subsequent leakage of emails from the Democratic National Committee and Hillary Clinton campaign, and the targeting of election infrastructure and local election officials in an attempt to interfere with the election.2

August: FIN7 Cyber Crime Group
Ukrainian nationals were indicted for participating in a prolific cyber crime group widely known as FIN7. They were accused of engaging in a highly sophisticated malware campaign that resulted in the theft of millions of customer credit and debit card numbers.3

September: Financial Institutions Hack
The U.S. Department of Justice announced the indictment and extradition of a Russian hacker accused of participating in the hack of JP Morgan Chase in 2014, leading to the theft of data from over 80 million customers, “the largest theft of customer data from a single U.S. financial institution in history.”4

September: North Korea Sony Hack
The U.S. Department of Justice announced the indictment of Park Jin Hyok, a North Korean hacker allegedly involved in the 2014 Sony hack, the 2016 theft of $81 million from a Bangladeshi bank, and the WannaCry ransomware attacks.5

Sources:
2. United States Department of Justice (August 1, 2018). Three Members of Notorious International Cybercrime Group “Fin7” In Custody for Role in Attacking Over 100 U.S. companies.
4. United States Department of Justice (September: North Korea Sony Hack
5. United States Department of Justice (July: Islamic Revolutionary Guard Corps

Learn more at: www.FireEye.com