The Corporate Consequences of Cyber Crime: Who’s Liable?
Introduction

Dennis Chesley, the Global Risk Consulting Leader for PwC, said that "many executives are declaring cyber as the risk that will define our generation." IDC predicts that one of every four people on Earth will be affected by a data breach by 2020. Yet a recent Nasdaq report found that “91% of Board Members at the most vulnerable companies can't interpret a cybersecurity report.” Given that breaches doubled in 2016, the knowledge gap between executives and IT must be bridged.

Companies have responded to these attacks with various tools, such as anti-virus, malware and other endpoint protection, intrusion detection and prevention systems, and others. But despite these additions, data breaches have been increasing steadily over the past five years. This means that either the attackers are improving faster than multibillion dollar security vendors, or that traditional security mechanisms aren’t enough anymore to protect enterprise data. Without direct visibility into the IT environment, non-technical executives can only trust in their technical leadership to guide them in the right direction when it comes to how to safeguard their systems.

But the fallout from data breaches and the responsibility for their consequences tends to be placed on executive leadership. This makes sense, since a customer establishes trust with a company, not a company’s IT department; therefore, failure to uphold that trust falls on those responsible for the company, not those responsible for firewalls and antivirus.

Executive Fallout in the Real World

The following examples show the precedents that have already been set regarding corporate responsibility for damages from cybercrime. These only represent the tip of the iceberg for what litigation and rulings the future will hold, as online business expands, bringing new risks to companies, customers and executives.

Executives Fired or Resigned as a Result of Hacks or Breaches

1. Target CEO Gregg Steinhafel Fired
   Target’s huge data breach affected over 40 million customers and contained sensitive payment card information. It was a huge blow to the company’s reputation and Target’s board, under pressure themselves as
culpable, asked for Steinhafel’s resignation. According to Forbes, the cost to Target for the data breach incident “will be in the billions by most estimates.”

2. **Sony Co-Chair Amy Pascal Steps Down**
The Sony data breach still makes headlines today, with journalists combing through the leaked correspondence and documents for stories. This data breach put Sony in the spotlight and humiliated many of its employees by revealing private communications that conflicted with the company’s slick PR efforts. When business communication is digitized, chatlogs, email, even text messages can be compromised.

3. **Austria’s FACC CFO Minfen Gu and Ceo Walter Stephan Fired**
A target of cyber fraud, aerospace parts giant FACC fired their CEO Walter Stephan and their Chief Financial Officer Minfen Gu after an attack cost the company 50 million euros, or 12% of their third quarter revenue. The scope of the consequences, number of records compromised, number of dollars lost, often determines the punitive reaction, even if everything else is the same. FACC stock rose upon the announcement of the CEO’s dismissal.

4. **Federal Office of Personnel Management Chief Katherine Archuleta Resigns**
A cyber attack compromised over 20 million records in the Office of Personnel Management (OPM) leading to the resignation of its chief, Katherine Archuleta. According to the White House press secretary, “new leadership was necessary for the agency to move forward, respond to the data breaches and implement steps to mitigate future risks.” This “necessity” seems to be independent of actions taken by leaders during their tenure, as the White House press secretary also said “It’s precisely because of some of the reforms [Archuleta] initiated that this particular cyber breach was detected in the first place.”

5. **Ashley Madison CEO Noel Biderman Resigns**
When dating site Ashley Madison faced extortion by hackers, CEO Noel Biderman refused to play ball. Not only did this lead to the publication of private Ashley Madison customer data, but Biderman's own personal email, revealing secrets of his own. Not long after, Biderman stepped down with “mutual agreement” from the board. For Ashley Madison, privacy is their product, and thousands of humiliated customers and uncountable potential customers will probably never associate themselves with that brand again.

6. **The State Of Utah’s CTO Stephen Fletcher Resigns**
Utah’s Department of Technology Services faced a breach that compromised 280,000 Medicaid records, including social security numbers. In response, Governor Gary Herbert accepted CTO Stephen Fletcher’s resignation and will be performing “an independent IT audit.” What makes this case particularly bad is that the “hack” was “a default password within the user authentication layer of the system.”

7. **The State off South Carolina’s Revenue Chief Jim Etter Resigns**
A data breach of state tax records
compromised the information of almost 4 million individuals and 700,000 businesses, causing revenue chief Jim Etter to resign and “get a new set of eyes on the department.” Yet, the cause of the data breach was an email phishing scam that a Department of Revenue employee fell for, giving their password to the hackers. When it comes to data breaches, the fallout for executives matches the effect of the breach, not its cause.

8. **Governor of Bangladesh’s Central Bank Atiur Rahman Resigns**
   One of the most massive cyber heists in history, 2016’s attack on the Bangladesh Central Bank resulted in $81 million stolen by hackers. The loss could have been ten times bigger, but a typo in one of the transactions drew suspicion that caused the remaining transfers to be canceled. The governor of the bank, Atiur Rahman, whose “main focus at the central bank was on poverty alleviation,” resigned in the wake of the incident.

9. **HBGary Federal CEO Aaron Barr Resigns**
   HBGary Federal, now operating as CounterTack after being purchased by that company in 2015, is best known for a highly publicized spat with hacktivist group Anonymous, in which thousands of the company’s private emails were compromised and put online after a claim that they had infiltrated Anonymous. This disastrous series of events led to CEO Aaron Barr’s resignation and the evisceration of HBGary Federal’s reputation as a security firm.

10. **Ohio University CIO William Sams Resigns**
    “Five separate security breaches, including one that exposed personal information on 137,000 people” hit Ohio University in Athens, causing then CIO William Sams to resign. According to an independent audit, “a siloed culture and a quasicombative relationship between the university’s network and computer services groups as reasons for a relative lack of good security practices.”

**Companies Sued After Hacks or Breaches**

1. **University of Central Florida**
   After a security breach compromised 63,000 people’s personal information going all the way back to the 1980s, former graduates filed suit against the university, claiming that it did not take appropriate measures to protect against the breach. This comes despite efforts by the university to provide credit monitoring services for affected people.

2. **Premera Blue Cross**
   At least five separate class action lawsuits were filed against Premera Blue Cross after a data breach potentially compromised millions of records. The healthcare industry has experienced more data breaches than any other sector and the legal and financial implications of that are just starting to unfurl. Some of the suits also claim that Premera did not handle the breach disclosure correctly. Even once the breach has occurred, companies can still compound the problem by mishandling the response.

3. **Wyndham Worldwide Hotels**
   Three breaches from 2008-2009 cost...
Wyndham Worldwide millions of dollars in fraud losses and compromised hundreds of thousands of customer records, including payment card information. The lawsuit in this instance was actually filed by the Federal Trade Commission (FTC), who claimed that Wyndham’s “privacy policy misrepresented the security measures the company and its subsidiaries took to protect consumers’ personal information.” Wyndham’s problems were multiplied when they failed to implement sufficient security measures after the first breach, giving the FTC more of a case for negligence.

4. Equifax
When a data breach disclosed the personal information of 431,000 Kroger employees, Equifax got slapped with a class action lawsuit that claimed they ignored known weaknesses within their systems. The justification for this claim is simple: they had been attacked in a similar way before and did not take sufficient steps to fix the problem. Most companies hope to never experience a single data breach like this, but when there is a pattern of breaches, it makes the case for company/executive responsibility much stronger. This is in part why an executive or two is often let go in reaction to these incidents: so the company can say they did something to address the situation. Unfortunately, if another breach happens under new leadership, it becomes clear that the problem still has not been addressed correctly.

5. Anthem Inc.
In one of the largest breaches in history, healthcare giant Anthem had over 80 million records compromised by a “sophisticated cyber attack.” One patient whose records were among those taken sued Anthem for damages. Litigation is often the only recourse customers have when a business is responsible for the loss of their personal information. And even a single lawsuit can be costly if that business is found responsible for the breach.

6. VTech
VTech, “the world’s leading manufacturer of children’s electronic learning products,” faced a breach in late 2015 that compromised the records of nearly 5 million people. Customers initiated a lawsuit against VTech, claiming that they “failed to secure and safeguard its customers’ personal information and failed to properly inform people that their information was hacked by an unauthorized individual.” This litigation extends the reputation damage done to the company and keeps people associating their brand with a data breach incident. On top of that, the financial costs of a class action lawsuit could be astronomical.

7. Wendy’s
A recent hack at fast food chain Wendy’s may have exposed “millions of customer credit cards.” Like the others, the lawsuit brought against Wendy’s claims that they did not take proper steps to secure their environment and protect against data breaches, even claiming that Wendy’s failed to follow established regulations for the handling of payment card information. PCI compliance assists businesses in protecting that data, and while compliance doesn’t guarantee security, non-
compliance speaks volumes in the wake of a data breach.

8. **T-Mobile/Experian**
   15 million T-Mobile customers had their data compromised when information housed on an Experian server was accessed by malicious parties. Even though it was Experian’s lack of security that led to the breach, T-Mobile still faces legal action for the incident, because they “misled the plaintiffs into believing that their sensitive information would be protected.” Most customers believe they have a reasonable expectation of privacy when engaging businesses. Failure to maintain that privacy can be interpreted as a breach of contract under certain conditions.

9. **Community Health Systems (CHS)**
   Another huge healthcare breach, this time compromising over 4.5 million records, hit Community Health Systems, a hospital corporation. For this, they were served a class action lawsuit by representatives of the patients whose information was taken. Even the FBI was moved to issue a warning to the healthcare industry after the incident regarding breaches.

10. **Excellus (Blue Cross Blue Shield)**
    One more healthcare breach involving millions of records was the Excellus BCBS breach of 2015, which has brought upon them a class action lawsuit claiming negligence and breach of contract. Again, previous breaches were used as an indication that the company should have improved its cybersecurity practices, knowing they were targeted for information theft.
Conclusion

A data breach is more than an IT problem. It’s a fundamental problem in the way business intersects with technology. On the one hand, technology has drastically increased the speed and scale of business, while on the other hand, the specialization necessary to understand this technology has created a silo within many companies managing critical business processes and responsible for important company and customer data. When these data or processes are compromised, business consequences result, including reputation damage, which is often handled by the firing of a top executive to show the public the company recognizes its mistake and is taking a new direction. Internally, a company may react by implementing even more security measures, but as mentioned above, that hasn’t slowed the rate of breaches.

Mending the disconnect between IT and business leadership requires a way to efficiently communicate IT issues and needs to executives, and business needs and strategies to IT. As it stands right now, most executives are totally in the dark when it comes to cyber security. Nasdaq reports that “98% of the most vulnerable CIOs are unaware of the steps to take action to prevent, locate, and neutralize cyber threats.” If a CIO is unaware of cyber threats, how much can other executives be expected to know? Likewise, IT teams find it incredibly difficult to communicate strategy, problems and needs up the ladder. This difficulty makes unfunded IT projects almost a cliche in the industry, with other priorities often edging out IT budget proposals. Just as much as upper management needs critical information about how their cyber infrastructure affects the business, so does IT need to give them that information to bolster their requests for resources. An IT operations team needs visibility into their environment, but a business also needs visibility into its IT operations, to prevent a single silo from disrupting the entire organization.
References


http://www.csoonline.com/native?prx_t=oxQCAtQsGAYwIMA


http://www.forbes.com/sites/ericbasu/2014/06/15/target-ceo-red-can-you-be-red-if-your-company-is-hacked/#4692176b7bc1

http://money.cnn.com/2015/02/05/media/amy-pascal-resigns-sony/

http://www.reuters.com/article/facc-operations-managementchanges-idUSL8N15I16G

http://www.reuters.com/article/us-facc-ceo-idUSKCN0YG0ZF


http://uk.reuters.com/article/uk-usa-fed-bangladesh-governor-idUKKCN0WH0H9


http://www.modernhealthcare.com/article/20150327/NEWS/150329913
Businesses depend on trust, but breaches and outages erode that trust. UpGuard is the world’s first cyber resilience platform, designed to proactively assess and manage the business risks posed by technology.

UpGuard gathers complete information across every digital surface, stores it in a single, searchable repository, and provides continuous validation and insightful visualizations so companies can make informed decisions.