Case Study

FTC v. WYNDHAM

EXPOSING COMPANIES TO DECADES OF GOVERNMENT OVERSIGHT
INTRODUCTION:

The frequency and damage caused by data breaches has increased dramatically in recent years. Businesses that are still not following well-established data protection measures leave themselves open to more than just the carnage caused by a data breach itself. As shown by numerous examples, victimize businesses are now also characterized as ‘part of the problem’, and are being treated as perpetrators by regulatory groups and law enforcement.

After it had been successfully attacked on three separate occasions, exposing over 600,000 records containing sensitive customer data, Wyndham Hotels found itself as a defendant when the Federal Trade Commission (FTC) brought federal charges, accusing the hotel chain of failing to protect its customers from third party data breaches.

In the end, after millions of dollars spent on attorneys and even more lost via operational disruption, the company buckled, agreeing to a consent decree that exposes it to continued legal action that will haunt the organization for the next two decades.

Through researched examples and the FTC v. Wyndham Hotels case study, this white paper discusses the potential risk factors associated with the C-Suite’s attention and actions, or lack thereof, toward cyber security as a corporate initiative.

THE DOUBLE CYBER THREAT TO THE C-SUITE

THREAT #1: YOU ARE A VICTIM… BUT OF WHAT, EXACTLY?

As so eloquently stated above, by former FBI Director (and current acting special investigator) Robert Mueller, it’s not a matter of IF, but WHEN you’ll be hacked, and it has probably already happened. The 2017 Verizon Data Breach Intelligence Report (DBIR) 1 puts it another way:

“If you haven’t suffered a data breach you’ve either been incredibly well prepared, or very, very lucky… are you incredibly well prepared?”

As with any instance of a cyber security event, there is an “attacker” and a “victim”. Numerous organizations and individuals are now perpetrating attacks, each with differing objectives. Attackers see many medium and large U.S. businesses as especially enticing targets, as they possess multiple types of valuable digital assets.

The Verizon DBIR defines attacker motivations, or “threat actor categories”, within 4 groups: 1) Financial 2) Espionage 3) Fun, Ideology, and Grudge (FIG) and 4) Everything Else. Understanding this is an effective instructional first step for determining the type of protection to prioritize for your organization.

---

1 Verizon DBIR, Published Q1 2017.
Figure 1 shows the trends that these various attack ideologies have followed during recent years:

**Figure 1 — Threat Actors Over Time**

Businesses are particularly prone to attack due to the fact that many of them are potential targets for all three of the top ideologies.

- Cyber criminals seek to reap the financial rewards from successfully obtaining sensitive information, such as customer credit cards and access to the accounting department's banking credentials.

- Nation state and competitive attacks seek to unearth important intellectual property via espionage-driven attacks, either your own IP or that of your partners.

- Other attacks are launched just for fun, or per the motivations of an ideology or grudge. These last two often involve insider threats from disgruntled or former employees with an axe to grind, or activist organizations that may disagree with certain business practices that your company employs.

Following the year (2016) in which the greatest recorded increase in cyber-attacks has occurred (38% YoY, according to PWC's Global State of Information Security Survey Report — GSISS), there is a danger of corporate numbness that can set-in. In other words, businesses fall victim not just to attackers, but also to complacency and lack of focus on cyber security basics. Here are some sobering statistics gathered from the most recent Verizon DBIR and PWC GSISS reports:

- 1 in 14 users falls victim to a phishing attack, clicking the bogus links that lead to immediate machine infiltration. This points to a need for increased security awareness among employees.

- 95% of phishing attacks result in malware being installed on the victim's end-point device. If end-point devices are not protected with anti-malware detection tools, your organization is at risk.

- 80% of hacking-related breaches leveraged either stolen passwords and/or weak or guessable passwords. Solid password techniques are essential in today's connected world where so much data is stored externally within password-protected applications.

- 61% of companies victimized by attacks are those with under 1,000 employees. Don't think for a minute that you are safe because you are not a large enterprise.

- 100% of data stolen and effectively used to commit fraud was unencrypted, and therefore easily used by cyber criminals. This is, by far, the easiest but often most overlooked data protection measure that you can take.
THREAT #2: YOU ARE A PERPETRATOR (“BUT WAIT, WE WERE THE ONES BREACHED!”)

On top of the damage caused as a victim of a data breach, your organization may be open to risk of being seen as a culpable perpetrator. Over recent years, the availability of defensive measures, tools, and techniques has become mainstream. Likewise, the expectation among consumers, business clients and government agencies that your company will employ these measures has also increased.

The FTC has emerged as a major force in regulating business’ cyber security measures and protecting consumers and clients through its policies. And the FTC is not alone... if your business transacts with government departments or foreign businesses, you may also be under the watchful eyes of the Department of Homeland Security, the CIA, and the NSA.

This is not new... as far back as 2010, the FTC started informing organizations that personal information, including sensitive data about customers and/or employees, had been shared from the organizations’ computer networks and was then made available on peer-to-peer (P2P) file-sharing networks by attackers who were seeking financial or ideological gain. In 2010 alone, the FTC informed over 100 companies about this activity, and started establishing guidelines leading to today’s policies and legal sanctioning authority.

These regulatory organizations have the power and legal authority to enforce cyber security standards, and impose sanctions and hold businesses responsible when it is found that they are not well-prepared to protect their customers and trading partners. In other words, while you are scrambling to mitigate the damage caused by a data breach, you may also find yourself defending against regulatory bodies that will dissect your cyber security strategy and tactics (if they exist) and seek reparatory actions and consent decrees to be enacted at your expense.

This may seem unfair, but it is proving to be an effective method of finally breaking through the complacency of the “it won't happen to us” C-Suite mind set. Unfortunately, this is something that did not sink in among the executives at Wyndham Hotels, as detailed in the following case summary.

CASE IN POINT: FTC vs. WYNDHAM HOTELS

A major hospitality company, Wyndham Hotels franchises and manages hotels worldwide, using a common property management system to collect customer information. Until recently (and we must hope that it is STILL not the case) most of this information was not encrypted. Between 2008 and 2009, malicious hackers accessed 619,000 Wyndham customer accounts, including their credit card information. Resulting fraud losses exceeded $10 million.

The FTC sued under section 5, alleging unfair and deceptive practices. When the district court denied Wyndham’s Motion to Dismiss, the hotel appealed. On appeal, the Third Circuit federal appeals court issued a sweeping precedent, ruling unanimously that the FTC had legal authority to enforce cyber security standards and hold companies like Wyndham responsible for their failures.
REVIEW OF FTC ALLEGATIONS:

In the federal complaint, it filed against Wyndham, the FTC set forth essentially seven cyber security failures:

Accusation #1 Wyndham allowed non-encrypted customer credit card information to be stored in clear, readable text.

Accusation #2 Wyndham employed easily-guessed passwords to access its property management system which contained private consumer information.

Accusation #3 Wyndham failed to use readily-available security measures to protect private consumer information.

Accusation #4 Wyndham failed to adopt and implement adequate cyber security policies and procedures.

Accusation #5 Wyndham failed to restrict access to its computer networks and servers from third party vendors.

Accusation #6 Wyndham failed to employ reasonable measures to detect, prevent, and investigate unauthorized access to its computer networks.

Accusation #7 Wyndham failed to adopt and follow adequate incident response procedures after it was hacked and knew or should have known of its vulnerabilities.

THE CONSENT DECREE ENTERED AGAINST WYNDHAM:

Wyndham could not win, or the risk was too great, so it buckled and accepted the FTC’s powerful consent decree. Lasting for 20 years, not to expire until the mid-2030s, the decree set forth three primary obligations:

Decree Obligation #1 Establish and implement a Comprehensive Written Information Security Program (WISP),

Decree Obligation #2 Conduct annual Risk Assessments of Compliance with its WISP, and

Decree Obligation #3 Maintain records of its decree compliance efforts, including assessments, audits and policies which the FTC may readily monitor and access to ensure diligent compliance.

LEGAL IMPLICATIONS OF THIS PRECEDENCE SETTING DECISION:

Implication #1 The FTC is now positioned as the prime federal regulator of corporate and consumer data security standards. “This settlement marks the end of a significant case in the FTC’s efforts to protect consumers from the harm caused by unreasonable data security,” said FTC Chairwoman Edith Ramirez after the decision was handed down. “Not only will it provide important protection to consumers, but the court rulings in the case have affirmed the vital role the FTC plays in this important area.”
Implication #2  The Third Circuit's decision elevates the importance of meeting FTC Guidelines in setting company cyber security operational standards for what will be considered reasonable or unreasonable data and information security. These Guidelines were cited by the court to prove the company was on notice of the law and as minimum measures for judging cyber security compliance in the future.

Implication #3  This ruling unequivocally establishes that companies can be both victims and violators, not only exposing them to the costs associated with loss of data, but also opening the flood gates for: (a) the FTC and other federal agencies to assert their regulatory and enforcement power in the cyber security world; (b) class action lawsuits by consumers over data breaches and unreasonable exposure to data breaches; and (c) SEC-based and other massive shareholder lawsuits based on unfair, fraudulent and deceptive practices (i.e., suggesting to the world you have reasonable cyber security systems in place for all data and information when you don't).

Implication #4  The Court emphasized that cyber security is not static; the obligation to provide reasonable cyber security protection is dynamic, aggressive, and ongoing. Companies must demonstrate reasonable commitment to securing information assets and consumer information with policy, systems, and training to mitigate the advancing threat. It is incumbent on companies to ensure policies and systems are vigilantly maintained and modernized to meet the latest threat, including education and training for all employees, from the lowliest clerk to the highest executive officer.

Implication #5  Cyber security protection must be the company's mindset. Cyber security cannot be an afterthought or secondary concern. It must be expressly budgeted, paid for, acquired, learned and implemented company-wide. This makes being able to prove affirmatively that all aspects of cyber security are in place, and that the company is diligently providing a cyber-secure environment 24/7, has never been more crucial.

LESSONS TO LEARN:

It's been over a year now since the Third Circuit handed down FTC v. Wyndham, ringing the legal alarm bell for cyber security inside the Board Rooms of America. Wyndham teaches hard lessons for companies and their counsel, both in-house and out. Here are some take-aways:

Take-away #1  You should encrypt sensitive data. This is one of the simplest and most commercially available methods for data protection in existence. There are new, innovative methods available for encryption that fit within your current business processes, and that do not require special training in cryptography.

Take-away #2  Establish and implement a rigorous WISP (Comprehensive Written Information Security Program) before some federal regulatory body makes you do so and actively monitors your security system for the next 20 years.

Take-away #2  Continually access, monitor and adjust your WISP considering all changing circumstances within your company and the world around you, including attacks your and other cyber-systems, cyber security incidents, cyber security breaches and the host of new technologies easily available to you.

© Copyright 2018 WikiLocks® All rights reserved.

Take-away #3  Be forever vigilant, as the FTC, other federal regulatory agencies, and state regulatory agencies all can level section 5 or section 5-like allegations against your company for failure to reasonably and adequately protect all data and information against cyber-intrusions, blaming you for your failure to reasonably protect private data and information even when you are also the victim.

Take-away #4  Learn, study, follow and vigorously implement all cyber security practices recommended, required, and detailed by section 5 and its substantial list of Guidelines, i.e., not complying with FTC guidelines could expose your company to significant cyber security incidents, breaches and consequent enforcement actions against you.

Take-away #5  Stay informed of, learn, study, follow and vigorously implement the standards set forth in all FTC consent decrees issued, using the decrees to shape your company's cyber security policies, procedures, and practices.

Take-away #6  Certain basic security measures (e.g., firewalls, encryption, access controls, vendor management, and incident response planning) should be considered standard for any reasonable data security program, whether the data is structured or unstructured. Companies that fail to meet these minimal standards could be subject to onerous actions by regulators and civil plaintiffs alike.

Take-away #7  Cyber security preparedness is a continuing obligation. Companies cannot sit back, wait or rest — because what may be a defensible posture today based on “industry standards,” will not be so tomorrow. Information security programs, methods of communication and protection, and both incident and breach response plans must be revised and adapted to the latest round of FTC guidelines, FTC decrees, and available technologies.

Take-away #8  Companies that experience a data security incident or breach must promptly identify and develop remediation plans to strengthen their overall security program and to reasonably prevent (or at the very least, promptly detect) a later breach where attackers use the same or similar methods. When this happens, it is essential to assess your entire cyber security program, as one failure often implies many others.

THE POST FTC v. WYNDHAM WAKE-UP CALL:

FTC v. Wyndham is the wake-up call, creating a prodigious challenge for many companies and organizations. You do not know when or how you will be hacked or breached next. But you do know it will happen. You also cannot identify every possible vulnerability because it is forever advancing, and you can’t entirely prevent it from happening. However, what you can do is vigilantly educate, train and modernize cyber security measures on a company-wide, ongoing basis (program maintenance).

The challenge is overcoming the mindset that you have already done this before and that your cyber security is adequate or reasonable. Companies must recognize that the threat is constantly advancing, and defences must be reasonably adequate to protect company assets and liability. And while it may appear to be an arms race in enhancements and updates to cyber security systems, policies and systems must be vigilantly supported and maintained. The threat persists 24 hours a day, seven days a week, 365 days a year. And what may be most important is that what is reasonable to you, may
not be reasonable to federal and state regulators, customers, business partners, and shareholders. The ultimate challenge, therefore, is staying ahead of the game wherever and whenever possible, by routinely auditing and reviewing your information security program, identifying vulnerabilities, establishing a cyber security program budget with contingency funds, and routinely exploring new for all employees and third-party contractors, and ensuring reasonable data and information security, particularly of sensitive data that may be breached or inadvertently shared outside of the organization.

WHAT DOES THIS MEAN TO YOU:

No matter what kind of sensitive information is involved, whether client or corporate, companies have and organization. The typical industry response is to lock the data down with more restrictive the latest methods and protocols for protection, education and training; and the most effective means for responding to, correcting, and remedying any prior security breaches. Put another way, it is time for every company to review and consider cyber security reform, making cyber security a way of life for all employees and third-party contractors, and ensuring reasonable data and information security. Anything less exposes the company to FTC v. Wyndham liability.

ABOUT WIKILOCKS:

As cyber-attacks are increasingly sophisticated and a persistent threat to every individual, business, and organization. The typical industry response is to lock the data down with more restrictive governance policies and security controls. However, when information assets are restricted, the effectiveness and efficiency of a business is significantly impacted. With information being the life blood of an organization, it needs to flow to customers, employees, and business partners. This challenging misalignment of security to business process leaves us with either too much or too little security. The industry lacks a solution that addresses the protection of the content, “the data”... Until Now!

WikiLocks is an innovative content security platform that allows for the movement and sharing of information without altering the way you do business. WikiLocks simply applies encryption to specific portions of sensitive content within unstructured data formats such as documents, emails, text, and images. Business and individuals can now allow information owners to properly classify and protect their sensitive content to protect the business. Using a simple “Select—Protect—Distribute” philosophy, WikiLocks leverages the user’s knowledge and skills of the most common business applications to protect content such as personal identifiable information, company secrets, or client-attorney privileged information to dynamically enhance the privacy and security of your business.