March 9, 2019

2019 OUTLOOK

The State of Cybersecurity

As cybercrime continues to increase, firms are devising more unique ways to address the privacy and safety concerns of businesses and consumers. This report will discuss the four primary categories that cyberattacks fall into as well as the motivations behind these malicious attacks. It will then provide an overview of recent regulations that the EU and the US have implemented to address the increasing concerns of cybercrime. After providing an overview of the cybersecurity space, the report will discuss the following:

1. As cybersecurity threats become an increasing concern, firms are committing further investment, research and development to implement preventative actions to prevent future attacks
2. Firms are implementing one of two types of strategies for the integration of cybersecurity products

While firms are pursuing various defense mechanisms to bolster their cybersecurity capabilities, cybercrime is expected to continue to increase into the foreseeable future. In response to this, the global cybersecurity industry has become increasingly competitive with key industry players leading the innovation of products in the market. Threats will continue to become more advanced and specialized through 2019 as technology evolves. Cybersecurity providers will need to ensure that they are advancing at similar, if not faster, rates to address these increasingly sophisticated attacks.

LIMESTONE CAPITAL

TMT Sector Team

Shawn Kang
Sr. Portfolio Manager

Jessica Galli
Sr. Portfolio Manager

Edward Huang
Analyst

Dylan Rupnow
Analyst

Michael Donovan
Junior Analyst

This report is for informational purposes only, and is not an offer to buy or sell or a solicitation to buy or sell any securities, investment products or other financial product or service, or an official confirmation of any transaction.

Overview of Cybersecurity Space

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. For sizeable organizations, this involves multiple layers of protection designed to keep critical information and data safe.

Over the past three years, the number of cyberattacks aiming to infiltrate the computer systems of corporations, governments and everyday civilians has risen dramatically. As these attacks become more frequent, their complexity and uniqueness are increasing simultaneously. Currently, there are five types of cyberattacks commonly used, as outlined in Figure 1.

Fig 1. Common Types of Cyberattacks

Type of Attack	Description	Notable Occurrence
Malware	▪ Uses software to gain unauthorized access or cause damage to a computer ▪ *Ransomware:* aims to extort money from victims	Windows *May 2017, WannaCry Attack*
Phishing	▪ Tricks people into revealing sensitive information through fraudulent and deceptive communication	*Attacks occur every minute*
Man-in-the-Middle *(MitM)*	▪ 'Eavesdropping' attacks, where hackers insert themselves into two-party communications ▪ Cybercriminals then steal the intercepted data	EQUIFAX *September 2017 Breach*
Denial of Service *(DoS)*	▪ Floods systems and servers with traffic to exhaust resources, preventing the system from fulfilling legitimate requests and effectively 'blocking-out' users	GitHub *March 2018, 1.3 Tbps Attack*
Zero-Day Exploit	▪ Exploits a network vulnerability *after* it is publicly announced but *before* a solution is implemented by the victimized company	chrome *March 2019 Attack*

Motivations of Cybercriminals

There are six key motivators that drive cybercriminals to conduct malicious attacks. The first three, money, ego and social status, are the easiest to identify. Many skilled coders and software engineers alike turn to cybercrime as a source of income and self-assurance.

The next key motivator is entertainment. Many hackers seek to interfere with people's lives or humiliate innocent civilians for personal enjoyment. For instance, in July 2015, a group called 'The Impact Team' leaked 25 gigabytes of data from the online dating site 'Ashley Madison', leading to the humiliation of millions.

Other cybercriminals have also been motivated to promote a political, scientific or social cause. In 2008, for example, the group 'Anonymous' threatened to expel the Church of Scientology from the internet in retaliation of the church's belief system.

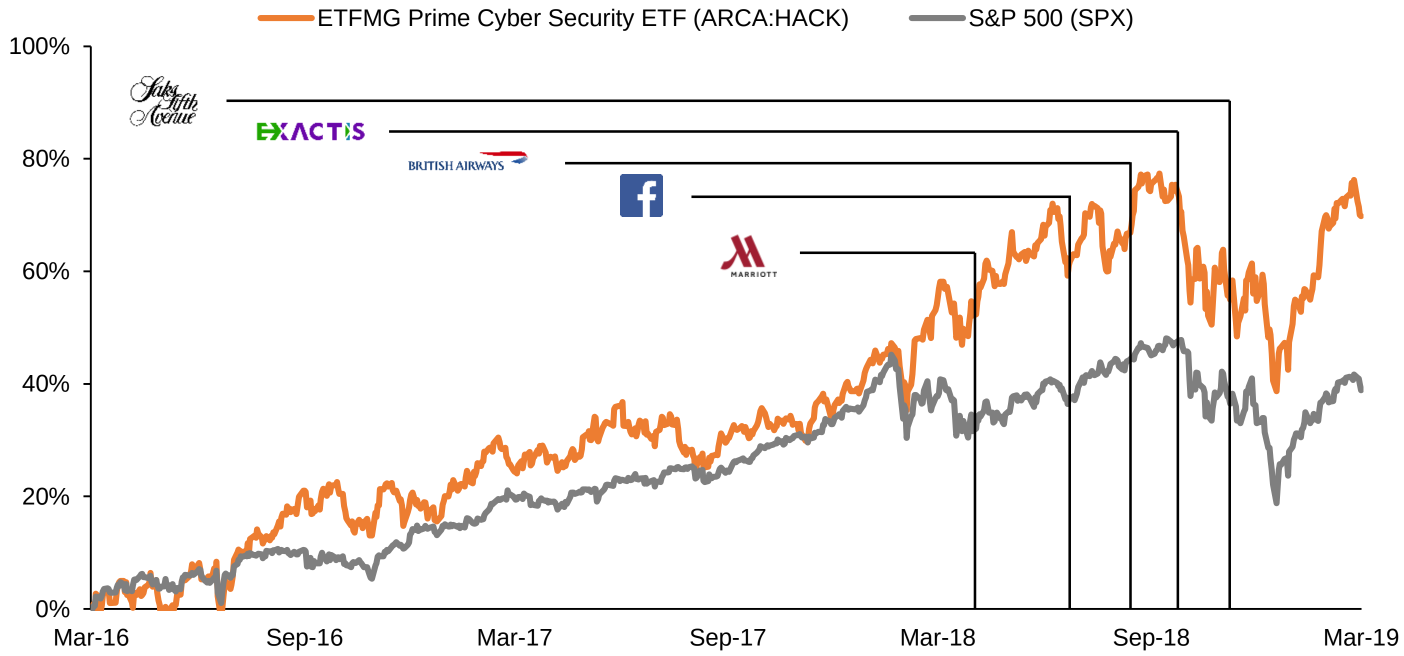
Lastly, many state-sponsored cybercriminals are motivated by power and influence when conducting cyberattacks.

Recent Developments in Cybersecurity Regulation

This past year, there has been a surge of cybersecurity breaches featured in the news. The EU was the first to pass a privacy regulation law through the institution of the General Data Protection Regulation (GDPR). California's upcoming compliance laws, set to go into effect in 4Q19, are expected to reduce the number of leaks plaguing companies, hopefully pressuring other states to follow suit. The laws require companies to disclose how they collect user data and how they plan to use it. Companies that do not comply will face hefty fines, damaging their financial position. The implementation of these new regulations will help diminish unnecessary data leaks. There have been a number of data leaks this past year that have been entirely preventable. These include MindBody, FedEx, Amazon, and Polar, each of whom had non-password protected servers. With new regulations enforcing data safety and companies facing monetary repercussions irresponsible behavior, we expect to see fewer exposed databases moving forward.

Cyberattacks Driving Growth Across Industry

Cyberattacks were a key driver of growth in the industry over the past three years. Nathaniel Fick, CEO of Endgame, phrased it, "every one of these attacks is a wakeup call that existing defences cannot withstand nation-state capabilities". Each time a breach occurs, further investment and R&D are needed to prevent the next one. Additionally, major companies that historically were not concerned about cybersecurity threats now have it as a priority. Examples include Saks 5th Ave. and Marriott. Both are relatively mature non-tech focused companies that are still impacted. This spurs investment in cybersecurity divisions across firms, thus driving revenues across cybersecurity players.



Defender Landscape: What are Companies Doing about Cybersecurity?

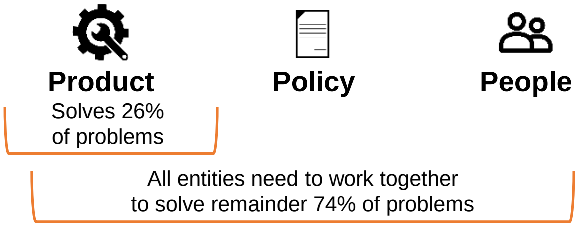
Types of Security Systems in Companies:
There are two types of strategies for integrating cybersecurity products. Companies can either utilize a “best-in-breed” approach, where companies employ different products that satisfy specific security needs, or an integrated approach, where one product handles all of a company’s security needs.

Currently, 72% of companies use a best-in-breed security system, and in that category, 57% of companies use it for cost-effectiveness and 39% use it because it is easier to implement. For the 28% of companies that use an integrated approach, the value proposition of these security systems centers around ease of implementation and cost-effectiveness.

Policies, People and Technology:

Only 26% of all cybersecurity problems can be solved using products alone. Most problems require policies, people, and products combined together to avoid these problems. Problems such as changing passwords to become more complex require all three aspects of cybersecurity. The people need to be trained to set up complex passwords, the products need to configure the servers and the policies need to be put in place to have certain requirements for what makes a password strong. It is the amalgamation of all three elements that makes a secure system.

Fig. 2: Products, People and Policies are equally as important for security


Product
Policy
People
Solves 26% of problems
All entities need to work together to solve remainder 74% of problems

Case Study: Marriott International Data Breach

Background:
The hotel industry has traditionally struggled to defend against cyber-attackers. With instances of complex credit card schemes, hackers taking control of keyless doors, and networks being hacked to spy on corporate executives, nothing topped the Marriott scandal that occurred in Fall 2018. Over 500 million accounts were hacked on the hotel’s network, exposing credit cards, passports, and other personal information. It was later confirmed that the cyberattacks were initiated in 2014 through the Starwood Hotels brand. Hackers were able to obtain access to the Marriott accounts because Starwood was acquired by Marriott in 2016.

Aftermath:
The breach was attributed to a Chinese intelligence group aiming to acquire more information about American citizens. Due to the weakness in the Starwood hotel system, Marriott has focused on phasing out the older system and transitioning to a newer one.

Implications:
Generally, there are no penalties enforced by the government following a data breach. The small instances of action taken by the SEC were minimal, and these penalties are not enough to push executives to take cyber risk more seriously.
Furthermore, the information breach was due to a weakness in an acquisition that Marriott made. Starwood’s entire IT department was laid off to cut costs, and as a result, did not provide Marriott any proprietary insight on how their security systems worked. This entire scandal could have been prevented if Marriott held a higher standard of security for the information systems at Starwood.

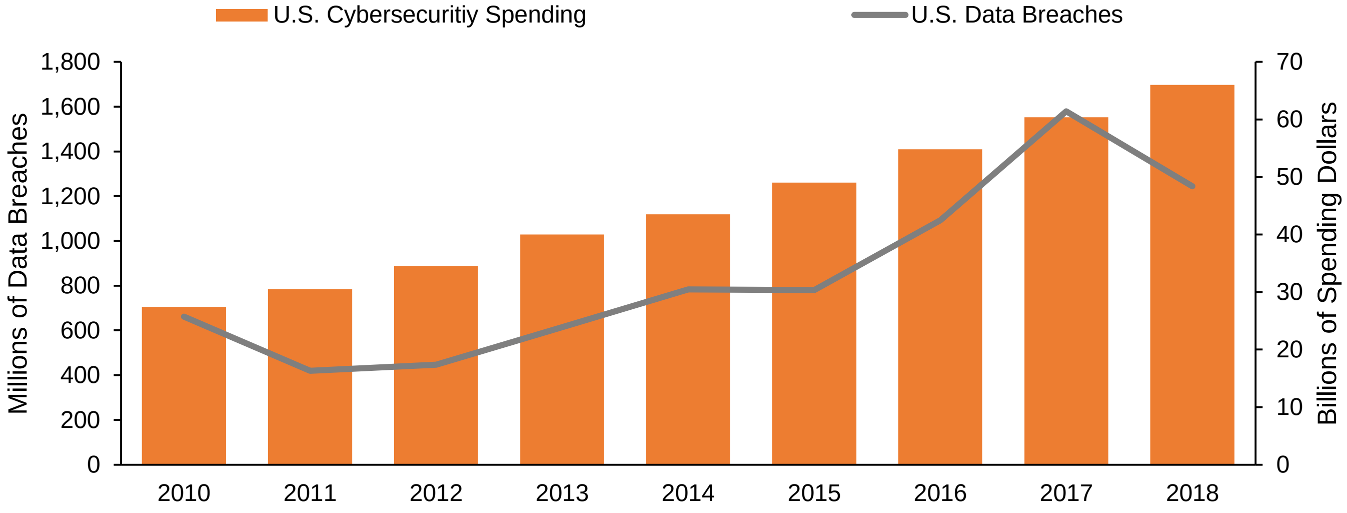
Rapid Growth of Cybercrime and Cybersecurity Markets Expected to Continue

Cybercrime rates have been increasing steadily over the past half-decade. Not only is the volume of data breaches increasing, the financial impact of cybercrimes on the world economy is also rising. According to a study by the Herjavec Group, cybercrime cost the world $3 trillion in 2015. This figure is expected to grow to $6 trillion annually by 2021, representing a 12.2% CAGR over the six year period.

Logically, increased spending by organizations on cybersecurity products has followed, with annual U.S. cybersecurity expenditure now totaling ~$67 billion. Over a similar time span, public equities in the cybersecurity sector have been steadily appreciating in value as well. The ETFMG Prime Cyber Security ETF, which tracks the top 50 providers of cybersecurity technologies, has returned +55% since its inception in November 2014.

Gartner, a world-leading research and advisory company, forecasts that worldwide spending on cybersecurity will top $124 billion in 2019. So long as cybercriminals continue to wreak havoc on a growing number of institutions, it is expected that growth in the cybersecurity industry will continue to follow suit.

Fig. 3: Growth in Both Cybercrime and Cybersecurity



Key Industry Players

The global cybersecurity industry has become extremely competitive, with a number of corporations offering a range of very similar technologies. Ten key players include:

1. **Symantec:** Provider of Norton Antivirus
2. **Intel:** Provider of McAfee software
3. **Hewlett-Packard:** Offers Security Risk Management & Digital Protection Services
4. **Cisco:** Range of offerings and a dedicated ‘Talos Security Intelligence Group’
5. **IBM:** Sells services of its X-Force Red blockchain cybersecurity unit
6. **Rapid7:** Offers ‘Insight’ line of products (e.g. InsightVM vulnerability management)
7. **FireEye**: ‘Innovation Cycle’ of offerings
8. **EMC RSA:** NetWitness Platform of products
9. **Sophos Ltd.:** Offers ‘NextGen’ firewalls
10. **Trend Micro:** Offers the ‘SMART’ Protection Network

Evolving Nature of Cyber Threats

As organizations push for more digitized operations to reduce costs and improve efficiency, they simultaneously become more vulnerable to cyberattacks.

The advent of sophisticated ransomware in 2017, as seen through the WannaCry attack on Microsoft Windows users, marked the beginning of the ever-changing cyber threat environment that exists today.

Four specific trends are anticipated to further evolve the nature of cyber threats in 2019:

Artificial Intelligence-Driven Chatbots

- Cybercriminals are expected to begin creating malicious chatbots that attempt to phish victims into clicking dangerous links, downloading nefarious files, or sharing private information
- Given the already-automated nature of chatbots, these attacks will be incredibly hard for everyday civilians to identify

Cyrptojacking

- Defined as the unauthorized use of a computer to mine cryptocurrency, this relatively undeveloped cyberattack seeks to insert a cryptocurrency mining ‘code’ onto a person’s device
- The ‘code’ then works surreptitiously to verify various cryptocurrency transactions and generate profit for the cybercriminal involved
- This type of attack is difficult to detect and easily accessible to the general public, with inexpensive cryptojacking kits available on the dark web

State-Sponsored Attacks

- Russia and the DPRK continue to exist as cybersecurity threats to major Western nations
- This modern form of cyberattack will be closely monitored in both Canada and the United States this calendar year for the countries’ federal and presidential primary elections, respectively

Attacks on Software Update Supply Chains

- Software updates have become the new target for cybercriminals, with many hackers now embedding malware into seemingly-harmless software updates on computer systems
- cyberattacks such as these prey on the vulnerabilities of these software updates, particularly given how unsuspecting people are of software updates being security risks

What to Expect in the Future: The Evolution of Malware

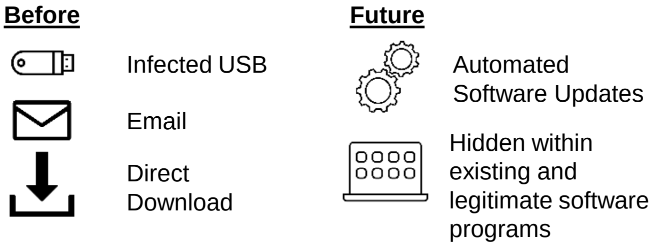
SamSam ransomware is a program that infects a network and encrypts massive amounts of data within that network. The hackers then request a payment (usually through Bitcoin) in exchange for the data to be decrypted. In 2018 alone, 56 organizations were attacked, with a focus on the Healthcare industry.

In 2017, the SamSam campaign quickly evolved and became stronger. WannaCry, another example of ransomware, took the internet by storm. Hackers in a group called the Shadow Brokers earned more than $143,000 through holding data hostage. Furthermore, there is no definite assurance that ransom payers will receive decryption codes.

The most worrisome recent development in ransomware was a virus called NotPetya, where hackers took advantage of a vulnerability in a tax software system in Ukraine. As a result, the virus was deployed through an automatic software update and was spread across more than 1 million computers.

In most cases, ransomware is generally installed through a hacker physically intruding into a company's network, manually installing a virus and then working remotely. With the evolution of malware accelerating, the biggest concern is the automation of malware.

Fig. 4: The spread of malware is expected to become automated without human interaction


Before
Infected USB
Email
Direct Download
Future
Automated Software Updates
Hidden within existing and legitimate software programs

Obstacles for Companies Improving their Cybersecurity

The costs associated with the aftermath of a cyberattack are substantial. With 53% of all attacks costing firms $500,000+, there are many other costs associated with cyberattacks. Having proper security is not just a source of protection, but an investment to reduce future cyberattacks.

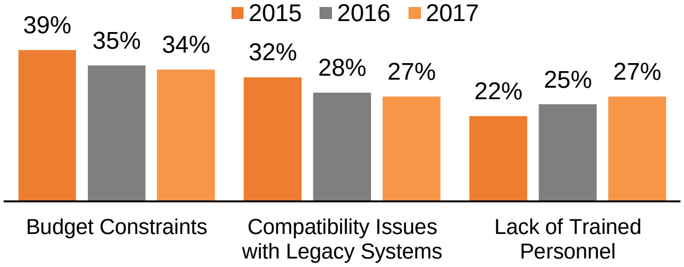
Furthermore, despite the consequences that can arise from cyberattacks financially, there are three main obstacles to a company implementing cybersecurity.

The main constraint is that companies fail to allocate capital to increase their cybersecurity. Considering the amount of monetary risk from cyberattacks, many firms fail to see the benefits of having a proper security system in place. This is a decreasing trend, as the importance of cybersecurity is becoming more widespread among executives.

The next constraint is integrating cybersecurity systems with legacy systems. The process of updating existing systems, implementing technology on top of IT platforms, and training staff can be arduous.

A growing concern is the lack of expertise in the industry. The median number of personnel in charge of cybersecurity is on the rise, however, increasing from 30 to 40 from 2013 to 2017.

Fig. 5: Main Obstacle for Implementing Cybersecurity according to Executives



References

I. CBC News

II. Cisco Systems, Inc.

III. CNET

IV. CSO Online

V. Cyberscoop.com

VI. Gartner Inc.

VII. Mirror Online

VIII. Statista

IX. TechCrunch.com

X. The Guardian

XI. The Herjavec Group

XII. Webopedia

XIII. Wired.com