CYBERSECURITY:

A COORDINATED EFFORT TO COMBAT THE GROWING THREAT

ext.

Leading financial services marketing

EXECUTIVE SUMMARY

Cyberattacks are making headlines around the world. The threat is real for all industries, especially financial services. As a result, more time and money is being allocated to finding efficient and effective cybersecurity systems. This shift in resources is essential to combat cybercriminals. Added up, there is now a coordinated effort from governments, regulators and business leaders.

Many businesses are required to implement cybersecurity and ensure all breaches are reported to the appropriate agencies. These measures are being used to develop standard best practices to minimize the threat of cyberattacks, and ultimately protect companies and their clients.

THE CURRENT LANDSCAPE

Cyberattacks are a major concern for financial firms, regulators and governments. Recent cyberattacks on Equifax, Yahoo! and Deloitte demonstrate the threats are real. In coming years, firms will be forced to allocate massive sums of capital to protect their information systems, whether from ransomware, phishing scams or application attacks. The challenge is staying ahead of the criminals.

What is cybersecurity?

According to *Digital Guardian*, cybersecurity refers to "the body of technologies, processes and practices designed to protect networks, devices, programs and data from attack, damage or unauthorized access. Cybersecurity may also be referred to as information technology security."[1]

Hackers attempt to bypass a cybersecurity system, while cybersecurity professionals are trying to stay ahead of them. This is no easy task. In a lot of ways, cybersecurity professionals are playing catch-up, trying to react with new measures and processes after a hacker has infiltrated a system.

The big fallout from a cyberattack

Cyberattacks result in businesses suffering serious

- Financial losses
- Legal action
- Reputational damage

Even if there are no financial or legal ramifications, the impacts on a company's trustworthiness and reputation could be catastrophic. Given the constant threat of cybercrimes and the vital importance of protecting people's privacy, it is not surprising that cybercrimes are on everyone's mind.

Cybercrime damage costs to hit $6 trillion annually by 2021.[2]

TAKING AN ASSERTIVE STANCE ON CYBERSECURITY

Governments and regulatory bodies have no choice but to take a more assertive stance on cybersecurity. Their proactive approach, while not 100% guaranteed to prevent another breach, does create a standard of care that companies can follow.

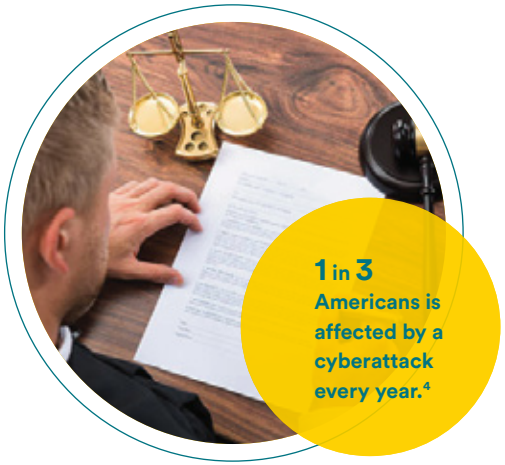
THE U.S.

U.S. regulators have taken thoughtful and significant actions to ensure financial services firms combat cyberattacks, even introducing privacy legislation. In fact, the U.S. has been the global leader in implementing mandates and legislation. This isn't surprising, given that U.S. firms are often the most targeted.

For financial services companies in the U.S., legislation pertaining to cybersecurity is set out in the *Gramm-Leach-Bliley Act, Bank Secrecy Act, USA PATRIOT Act*, the identity theft red flags rule and *Sarbanes-Oxley Act.*[3] To ensure compliance, these firms are regularly monitored, which results in a substantial level of accountability and diligence.

The U.S. Securities and Exchange Commission ("SEC") is also taking a tough approach with firms and their defense against cyberattacks. The SEC will hold firms accountable if they do not have an effective and up-to-date cybersecurity system in place.

Finally, the Financial Industry Regulatory Authority ("FINRA") has stressed the need for increased cybersecurity among its member firms. FINRA has mandated members to make cybersecurity a high organizational priority, while also issuing guidance on how to implement an effective cybersecurity program. FINRA monitors and reports on cyber breaches, hoping to engage and educate its members on the next threat and how to combat it.



CANADA

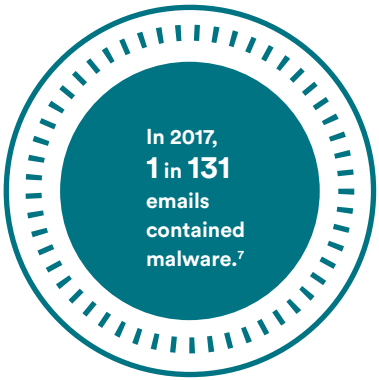
Data protection and cybersecurity are governed by a complex legal and regulatory framework. According to McMillan LLP, failure to understand this framework and take active steps to reduce risks (or the impact of such risks after they materialize) can have serious legal and financial consequences for an organization.[5]

Financial services firms work under the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). Under PIPEDA, financial services firms must take physical, technological and organizational measures to protect and secure clients' personal information. Failure to do so can result in significant fines and penalties. PIPEDA also demands that firms report any breaches of security where clients' personal information may have been stolen.

According to the Office of the Privacy Commissioner of Canada, firms should focus on three areas to protect clients' information:

1. Building privacy values into cybersecurity policy directions
2. Legislative approaches that incentivize cybersecurity preparedness
3. Facilitating broader dialogue on cybersecurity that acknowledges its importance for privacy, trust and responsible data stewardship[6]

Regulatory organizations for the financial services industry are also taking an active role in cybersecurity. They are providing guidance on how member firms can better protect themselves from cyberattacks, using best practices to do so. They continually stress the importance of cybersecurity and, by extension, client privacy, in order that their member firms will be more diligent with their cybersecurity measures.



INTERNATIONAL

Many countries and regions are implementing plans to fight cyberattacks and define their cybersecurity programs for businesses. This represents a coordinated effort from law-makers, regulators and businesses, including financial services firms, to put regulations and processes in place. Below are a couple of examples.

In the European Union, the Network and Information Security Directive ("NISD") has enacted cybersecurity legislation. The NISD will expect companies to follow certain cybersecurity rules and procedures, while forcing businesses to report any cybersecurity incidents. These incidents will be reported to the National Competent Authorities. NISD legislation applies to financial services firms, among others.[8]

In Australia, the government has taken a cooperative approach with businesses to fight cyberattacks. The creation of the Australian Cyber Security Centre allows government and businesses to work together to find effective solutions for cybersecurity and develop solutions to deter future cyberattacks. Australia is also putting significant resources behind heads of cybersecurity at the government level, additional training for law enforcement agencies to fight cybercrime, and education and development for individuals to enter the cybersecurity space. The Australian government has taken a leadership position to fight cyberattacks both nationally and globally.[9]

70% of Millennials admitted to bringing outside applications into the enterprise in violation of IT policies.[10]

OUR OPINION

The threat is real. Cyberthreats are clearly scary and unwanted, especially for financial services firms. The consequences of inaction could be devastating for clients and businesses.

Hackers are always looking for new, effective means to attack companies' information systems. Getting ahead of hackers and protecting information takes monumental work, but a coordinated effort among governments, regulatory bodies and companies would help reduce the number of successful cyberattacks.

Any legislation assisting or mandating cybersecurity measures should be viewed positively, as they are good for everyone – governments, regulatory bodies, companies and most importantly, customers. And they're bad for hackers.

As organizational bodies become more involved, they will make sure methods and processes are focused on preventing cyberattacks, not just reacting to them. This mindset – one that focuses on active prevention – has a positive impact on the implementation of cybersecurity.

Finally, governments, regulators and companies must work together to find solutions as no single individual or firm can stay ahead of these constantly evolving threats.

SOURCES

1 https://digitalguardian.com/blog/what-cyber-security

2 https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html

3 https://www.lw.com/thoughtLeadership/Cybersecurity-regulation-and-best-practice

4 https://www.cybintsolutions.com/cyber-security-facts-stats/

5 http://mcmillan.ca/Cybersecurity--The-Legal-Landscape-in-Canada

6 https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/cs_201412/

7 https://www.symantec.com/security-center/threat-report

8 https://www.lw.com/thoughtLeadership/Cybersecurity-regulation-and-best-practice

9 https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf

10 https://www.tektonikamag.uk/index.php/2017/06/22/35-cyber-security-statistics-every-cio-know-2017/

ADDITIONAL SOURCES

https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/evolving-investment-management-regulation.pdf

https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/06/evolving-investment-management-regulation-fs.pdf

https://digitalguardian.com/blog/what-cyber-security

https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security

https://www2.deloitte.com/us/en/pages/financial-services/articles/dcfs-transforming-cybersecurity.html

https://www.cgi.com/sites/default/files/SIBOS2015/cybersecurity_financial_services.pdf

https://www.pwc.com/gx/en/financial-services/assets/pdf/technology2020-and-beyond.pdf

http://www.bobsguide.com/guide/news/2017/Aug/21/the-cybersecurity-risks-to-financial-services-that-are-making-the-biggest-impact-in-2017/

https://sibos.societegenerale.com/en/2017-expert-views/technology-stream/cyber-security-trends-financial-services/

http://www.tfsa.ca/storage/reports/TrendsandInnovationsinFinancialServices2017.pdf

https://www.globalbankingandfinance.com/cybersecurity-the-financial-services-space-in-2017/

https://www.reuters.com/article/us-cyber-g7/g7-sets-common-cyber-security-guidelines-for-financial-sector-idUSKCN12B1UB

http://mcmillan.ca/Cybersecurity--The-Legal-Landscape-in-Canada

https://www.lw.com/thoughtLeadership/Cybersecurity-regulation-and-best-practice

https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20

https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/ZA_Transforming_Cybersecurity_05122014.pdf

https://www.symantec.com/content/en/us/enterprise/white_papers/cybersecurity-whitepaper-financial-wp-21352892.pdf

https://learningnetwork.cisco.com/blogs/talking-tech-with-cisco/2017/05/18/the-state-of-cybersecurity-laws-in-the-financial-services-industry

https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/cs_201412/

https://blog.appknox.com/glance-australias-cyber-security-laws/

https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf

ABOUT ext.

We are a full-service financial marketing agency that brings together agency creativity and deep industry knowledge to grow your firm's business.

Contact us today to find out how.

ext.

Leading financial services marketing

Toronto
34 King Street East, Suite 701
Toronto, ON M5C 2X8
416.925.1700

New York
450 7th Avenue, Suite 1400
New York, NY 10123
917.304.1900

1.844.243.1830
info@ext-marketing.com
ext-marketing.com