WHITE PAPER

Leveraging IT Infrastructure as a Service

enables agile response to constantly changing threats.

LUMEN℠

The number of cyber threats continues to grow exponentially in size and scope. According to Cybersecurity Ventures, “cyber attacks are the fastest growing crime globally, increasing in size, sophistication and cost … cybercrime damages will cost $6 trillion annually by 2021 — exponentially more than the damage inflicted from natural disasters in a year, and more profitable than the global trade of all major illegal drugs combined.”[1] As a result, Gartner forecasts worldwide information security spending to exceed $124 billion in 2019.[2]

This startling increase in the sophistication and number of cyber attacks is forcing virtually every company to rise to a level of security consciousness that would have seemed excessive or even paranoid just a decade or two ago.

That was then, before the words phish, spam, virus and trojan acquired new meanings and became part of everyone’s vocabulary. This is now.

According to Forbes, the financial services industry, "experiences 35% of all data breaches, earning it the unflattering title of the most-breached sector. It's easy to understand why. The industry is known for its wide array of interconnected systems and the processing of millions of transactions — factors that render it particularly vulnerable to attack".[3] Other concerning statistics from Forbes include:

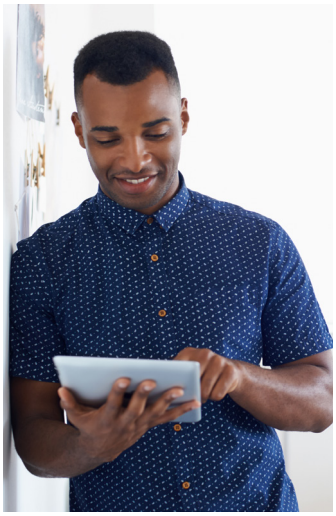
- Cyber attacks cost financial services firms more to address than firms in any other industry at $18 million per firm
- Financial services firms also fall victim to cybersecurity attacks 300 times more frequently than businesses in other industries
- Among financial services firms, banks lost $16.8 billion to cybercriminals in 2017. Attacks on SWIFT — the leading global network for money and security transfers — alone cost $1.8 billion year-to-date
- Denial of services and phishing and social engineering are the two most costly attack types for financial services firms
- 90% of financial institutions reported being targeted by ransomware[4]

Today, with so many potential attackers, it's hard to draw up a reliable short list so that you can start the process of planning your defensive strategy. It's even harder to thwart an attack if you don't know what an attacker might be trying to achieve. Is someone launching a distributed denial of service (DDoS) attack to shut you down for a few hours and create uncertainty among your customers? Or is that just a smoke screen for stealing credit card information? Or perhaps they're trying to overwhelm your ISP so they can slip behind the defenses of another ISP customer.

It's hard to say, especially because it's no longer enough to just look for a profit motive. The attackers may be trolling for intellectual property. Or they may be seeking to cause damage for their political benefit. Often attacks are not motivated by monetary gain but by nihilism, vandalism, politics or ideology, bragging rights, or a host of other motives.

Just as the landscape of potential attackers and motives keeps changing, so too does the arsenal of disruptive tools and techniques available to them. Today's adversaries are much more sophisticated than ever before, with access to more code and expertise than existed

just a few years ago. It's not enough for your organization simply to thwart an attack: You have to continually prepare for the next one even though you can't predict much about it — except that it's likely to be smarter and stronger than the one you've just survived. You need to build up a dynamic and proactive defensive capability that protects you from attack and increases the speed and agility of your response to any threat.



Raising the drawbridge is not an option

Financial services businesses — like organizations in all industries — have been outgunned by the hackers. Attacks are bigger and more sophisticated, and perimeters are more permeable than ever before. It's tempting to imagine walling off corporate systems, but current business practices won't allow it.

Cloud, social, and mobile technologies, including bring your own device (BYOD), are simply too cost-efficient and effective for institutions to ignore. And, as a services institution, you have to meet your clients' demands for easy access. In 2018, about 61 percent of Americans used digital banking, which is set to rise to 65.3 percent by 2022, according to Statista.5 In 2014, there were 133.5 million digital banking users in the U.S. and this figure is projected to increase to 161.6 million in 2019. There's no retreating from the levels of openness and access that customers have come to expect.

Your firm has already been infected

These days, every organization must base its security strategy on an acceptance that it is already infected with some form of malware, to some degree, with or without knowing it.

Because perimeters must be permeable to allow web server traffic to flow and employees to interface with customers and vendors, complete protection is impossible. Traditional defenses are still useful, from blocking and tackling to defense in depth. But you have to augment them by dealing with attack mechanisms that have infiltrated your business. You need to shift the focus of cybersecurity tactics from building walls to analyzing, detecting and expunging threats already inside your system. How can those be identified, stymied and removed?

Due to the complex kaleidoscope of attackers, motives and tools, these are difficult questions to answer. Yet the SEC — and your stakeholders — are going to be holding you responsible for doing so. SEC guidance is now that firms must declare any material risk to their networks, including:

- Aspects of your business or operations that give rise to material cybersecurity risks, and the potential costs and consequences of those risks.
- Functions that you outsource that have material cybersecurity risks, and how you address them.
- Description of cyber incidents you've experienced that are — individually or in the aggregate — material, including a description of the costs and other consequences.
- Risks related to cyber incidents that may remain undetected for an extended period.

This is a lot of responsibility for a firm to shoulder, so many banks have reached out to the United States government for help. Firms have banded together to pool resources and knowledge in the face of this common threat. Increasingly, even the largest, most sophisticated financial services firms — like businesses in every other industry — have

begun to realize that mitigation of security risks has become such a complex task that it's much like a separate line of business. Which raises the question every firm should ask itself: Do you want to be in the cybersecurity business? Is state-of-the-art IT security a specialty that you want — or can afford — to build in-house?

> **"High-profile data breach events have hastened stakeholder focus on the ways in which sensitive data is housed and whether management is taking a holistic and comprehensive approach to protecting the data."**
>
> **— Bloomberg Law Reports**

What is the next attack?

Today's threat environment comprises more attackers — and more tools — than ever before. It's impossible to describe all the tools and other resources that may be used to launch an attack on your organization, because the scope is expanding all the time. Criminal enterprise supply chains sell inexpensive software tools that can be quickly customized to suit the attacker's goals and avoid detection by systems. Commercial DDoS attack services and DDoS bots that combine high-volume bandwidth and low-volume application-level attacks are readily available and can be used to shut down your online services — and can also serve as a distraction while a more focused and stealthy attack takes place on your organization or on another organization that uses the same ISP. Public websites that your staff visits can be infected in a way that specifically targets your business. Well-crafted spear phishing emails can hook even senior and savvy employees. And new bots are continually evolving to be smaller, harder to detect, more effective and more organized, making them impossible to flush out of systems.

Where is the next attack coming from?

This continually evolving arsenal of tools is in the hands of a wide range of attackers, from shadowy organizations and individuals such as nation-states, criminals, hacktivists and terrorists to the most damaging attackers of all — well-known and even well-liked insiders.

Nation-states

Ongoing news has highlighted the cyberterrorist activities of nation-states motivated by political and ideological differences. The U.S. Department of Justice announced an operation to disrupt a North Korean botnet that had been used to target companies in the media, aerospace, financial, and critical infrastructure sectors. The U.S. Securities and Exchange Commission charged a group of hackers from the U.S., Russia, and Ukraine with the 2016 breach of the SEC's online corporate filing portal exploited to execute trades based on non-public information. North Korean hackers were found to have used malware to steal tens of millions of dollars from ATMs across Asia and Africa.

Cybercriminals

Criminals are everywhere — and cybercriminals are also nowhere, making them virtually impossible to catch. Young hackers are being offered large sums of money — and bragging rights — in exchange for taking on the challenge of bringing down major institutions. From incidents such as large-scale ransomware attacks Carbanak and Cobalt — an operation that has struck banks in more than 40 countries and has resulted in cumulative losses of over 1 billion euros for the financial industry — to ongoing attacks on cryptocurrency infrastructure (wallets, exchanges, etc.), 2018 saw the continuation of a challenging environment for IT security in its attempts to defend against cybercrime, with some estimates exceeding over $5 billion in damages.

Today's threat landscape

- 450,000 unique strains of malware deployed every day
- 4,000 ransomware attacks occur per day[6]
- 22,000 DDoS attacks launched daily
- 45% of DDoS attacks are more than 10 Gbps per second, 15% of attacks are at least 50 Gbps[7]
- There is a hacker attack every 39 seconds, affecting one in three Americans each year
- 3.8 million records stolen from data breaches every day

Hacktivists and cyber-terrorists

Hacktivists and cyber-terrorists, some sponsored by nation-states and others working only for themselves or small groups, are motivated mostly by the desire to destroy prosperity and stability. Security organizations track pending campaigns and warn that some of the threats on the horizon could be devastating to financial services firms.

Insiders

Insiders include current or former employees, contractors or other business partners who have or had authorized access to your network, system or data. Because they can bypass your security measures through legitimate means, they can misuse that access and knowledge to impact the confidentiality, integrity, or availability of your information or information systems. Privileged access enables insiders to inflict more damage than almost any other attacker. Sometimes, they do so unintentionally, through error or carelessness. But if managers in financial services organizations set out to commit fraud, studies show that their schemes tend to cost organizations twice as much as when non- managers instigate these crimes.

What does an attack cost you?

Some attacks are aimed at defrauding financial services firms. In these cases, it can be relatively easy to quantify the monetary damage your firm suffers. The time to respond and mitigate DDoS attacks can be costly for companies, and some businesses can lose roughly $2.5 million on average per attack.[8] But attacks can be even more damaging in ways that are less easy to measure.

Your firm's credibility suffers when customers experience downtime as a result of a DDoS attack. Your brand loses value. Customer satisfaction decreases, too, as some attacks can take a site offline — or reduce performance to a crawl — for hours. During that time banks often suffer losses in sales opportunities and revenue because they are unable to respond promptly to market conditions. Productivity takes a hit as well, as highly-paid employees are forced to idle, waiting for service to be resumed.

Long after the attack is over, your firm could still feel the effects of a loss of customer confidence. Your SMB customers view security as your job, not theirs.

What can your firm do for itself?

Like most financial services firms, you have probably already taken extensive precautions in-house. You've almost certainly locked down applications and servers, configured perimeter firewalls to block known network DDoS attacks, and implemented as many of the other 30 or so security best practices set out in various websites as you could afford to do.

But is that enough?

In every industry, firms are asking the same question — and in the high-profile, high-stakes world of financial services the question is even more urgent. Increasingly, firms are weighing the merits of buying IT security services, rather than trying to build (and maintain) their own. Today's constantly changing landscape of threats and rapid evolution of new technologies make it difficult for most firms to fend off attacks. Leveraging the scale and most importantly the expertise of IT security services providers offers your organization a way to gain higher-quality protection, more cost-effectively, than you could do on your own.

Buying IT security as a managed service

Depending on the provider and package, buying IT security as a managed service can provide your firm the hardware, software, infrastructure and, most critically, the information and expertise that you need to protect your business in today's complex and evolving threat environment. This is not a complete list, but it does cover some of the most important — and some less well-known — security issues to consider.

DDoS mitigation services should be at the top of your list of required services. Consider only those providers who can detect attack traffic on their or your network before it impacts your infrastructure. Providers should be able to divert traffic and cleanse it of malicious packets before forwarding it to your site. Services can be expensive, so look for one that charges only a low monthly retainer fee, plus an hourly charge for traffic cleansing, so you get protection but don't pay a large monthly premium for mitigation you may rarely need. You'll also want one that commits fully to standing by you in case of an attack, with skilled analysts who not only monitor the network for attack traffic, but also work with you 24/7 during an attack to deploy any available countermeasures to keep your site protected.

Web application protection can help your organization to cost-effectively protect its sensitive financial, human resources, and customer credit card data from

application-based attacks by detecting and blocking malicious web requests, learning the expected usage and monitoring activity of protected applications, and inspecting outbound traffic to ensure no data leakage — all with minimal latency.

Cloud computing security services are essential for your hosted or internal cloud. Your provider should secure your data through encryption and masking but allow you to remain in control of it. In order to buffer your infrastructure from the dangerous world that exists beyond your network, the provider should proactively identify attacks that can pose the greatest threats to your highest-value IT assets, filter out insignificant attacks so you can focus on the more critical ones and continually scan for internal vulnerabilities.

Log management may not seem like a front-line security issue, but it is important as the volume of log data you accumulate increases and as compliance requirements proliferate. There's a lot of work involved in collecting, analyzing and archiving IT logs. Look for a service that can cost-effectively assist your organization in addressing its compliance requirements, such as the PCI DSS requirement that any entity that processes credit card data must securely gather, analyze and archive specific log data, making it available online for 90 days and archiving it for 12 months. And to help you get value from that data, it should also provide an easy-to-use interface that includes a broad range of standardized reports as well as the ability to customize reports to meet your specialized requirements.

Network intrusion detection and prevention can help you keep pace with the growing volume of increasingly complex cyber attacks. Look for a service that will alert you when a critical threat that might have a significant impact on your security infrastructure appears and respond 24/7 with appropriate action based on your preferences. Even when no threat is on the horizon, you should seek a service that configures, monitors, and maintains intrusion detection and prevention (IDP) sensors, and provides ongoing detailed monitoring and reporting for a better view of potential problems and vulnerabilities.

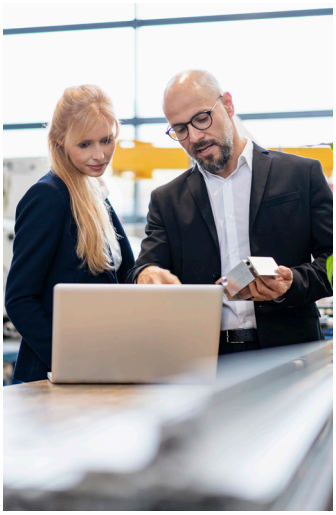
Data is quickly becoming the platform on which business success or failure is built. And your applications, from your external-facing web apps to your messaging apps, can be entry points to your organization and therefore play a critical role in helping to protect that data. It's been reported that software issues are responsible for 90 percent of IT failure and breaches. Lumen helps you protect your applications and data through a holistic approach that includes network encryption, email and web security, application code reviews and vulnerability testing, and data loss prevention programs.

For businesses weighing the advantages of an increasingly mobile workforce against the need to protect sensitive information in today's complex cybersecurity landscape, Lumen offers Adaptive Network Security Mobility, a network solution that enables remote users to securely connect to internet and private network resources without introducing cyber risks associated with using personal devices and unsecured WiFi.

Content integrity monitoring too often flies under the radar of internal security groups. But with some attacks focused on tampering with data in files, you need a service that helps you keep a constant watch on your mission-critical files and programs. Look for one that monitors critical directories and files residing on a host computer and alerts you whenever specified files undergo an unexpected change.

A state-of-the-art solution: Lumen℠ Connected Security

Lumen offers all the state-of-the-art services described in this paper — and more. Whether you want security protection delivered at your premises, within a Lumen data center or in the cloud, we've got you covered. Our services range from a basic firewall to comprehensive security coverage that includes threat management, DDoS attack mitigation, log management, web application protection, authentication and authorization services, and physical data center security.



When you select Lumen as your managed security services provider, we enter into an agreement with you, helping you assess your organization's unique risk profile and threat landscape, spelling out the protective measures available to you, and then working with you as you decide which security tasks you'd prefer to handle in-house and which you would like us to take on.

No matter which path you choose, you'll be able to tap into the extensive range of skills of our Corporate Security team. Security is not a sideline for us: it's the heart of our business, and we invest in it accordingly. We have staff focused exclusively on network security, physical data security, infrastructure, law enforcement, national security, fraud management, enterprise technology protection and enterprise security. Specialists in each of these areas interact to gain fresh perspectives on current, emerging and future threats to our clients. In addition, we are engaged in state-of-the-art information sharing and technology through public-private partnerships, including the FCC Communications Security, Reliability and Interoperability Council (CSRIC), and with the Department of Defense, Department of Homeland Security, FBI, and the White House.

Government and private-sector organizations worldwide must take responsibility for protecting cyberspace, and information sharing among these organizations is likely to grow. Lumen is positioned to be a key player in any such initiatives. The Lumen infrastructure serves more than 1,500 enterprise security clients and hundreds of financial services clients. With more than 5,000 security installations under management, and a track record of more than 15 years of delivering security, we have proven expertise in security for enterprise IT. And, unlike some vendors, we are completely technology agnostic. We adopt only best-of-breed products to address emerging threats.

Can you afford state-of-the-art security? Can you afford not to have it?

Growing a financial services business has always required cultivating customer relationships and decreasing churn. These days, security and customer confidence are critical to that effort — and your business' revenues. You should consider making security a prominent part of your marketing and outreach activities, to communicate to customers and prospects that you offer unparalleled security for their business.

To deliver the security customers demand of their financial services providers today requires expertise and resources that few firms have in-house. If you wanted to create state-of-the-art security in house, just keeping your equipment and software current would take up a huge share of your total IT budget.

Security technologies are expensive, and constantly changing. But that's not enough. You would also need to find — and recruit and retain — skilled security professionals.

These people are rare, and charge a premium for their services. You might choose to turn to your partners and third-party providers for assistance with security, but unless you can be certain of every member and every system within that larger ecosystem, you could be increasing your company's vulnerability rather than decreasing it.

Lumen infrastructure by numbers

- We monitor ~1.3 billion security events per day
- We identify over 267 and remove 35 new C2s a month.
- We track over 5,000 C2s per day
- We respond to and mitigate ~120 DDoS attacks a day
- We monitor over 114 billion NetFlor sessions per day
- We collect ~357 million DNS queries per day.

Lumen has the scale and resources to provide the world-class security your firm needs in order to maintain and grow its business in today's ever-changing and darkening threat environment — all at a commodity price. Call us today to start the conversation about how Lumen℠ Connected Security can help your organization protect itself — and its customers — from evolving internal and external threats.

Footnotes

1. 2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics, https://cybersecurityventures.com/cybersecurity-almanac-2019/
2. Gartner press release, August 15, 2018, https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019
3. "What Financial Services Executives Need To Know About Data Security", https://www.forbes.com/sites/insights-klgates/2019/01/15/what-financial-services-executives-need-to-know-about-data-security/#5f21c0af1e43
4. "Laughing All The Way To The Bank: Cybercriminals Targeting U.S. Financial Institutions", August 28, 2018, https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#183b5e3e6e90
5. https://www.statista.com/statistics/946109/digital-banking-users-usa/
6. "24 Cybersecurity Statistics That Matter In 2019", https://preyproject.com/blog/en/24-cybersecurity-statistics-that-matter-in-2019
7. Neustar Press Release, https://www.home.neustar/about-us/news-room/press-releases/2017/ddos2017
8. Worldwide DDoS Attacks and Cyber Insights Research Report, Neustar, May 2017

LUMEN℠