Preventing federal financial cyberattacks

Securing the intersection between high finance and government policy

Financial institutions today are a ripe target for cyberattacks. If you are a financial institution associated closely with the federal government, like Federal Home Loan Bank, Farm Credit Administration, and government-backed home mortgage companies like Freddie Mac, you carry even higher risk. Because you play a vital role in steering segments of the economy and setting policies that impact the direction of industries, you stand out as unique, high-profile targets for today's bad actors.

As attacks grow more sophisticated, a new arms race has erupted. Your approach to security must keep up – and even get ahead of the curve. Money, reputation and public trust are at stake.

> **Your approach to security must keep up – and even get ahead of the curve.**

LUMEN®

Threats and bad actors come in many forms

The landscape of threats for these government-affiliated institutions is growing and potential perpetrators come in many forms.

- Cybercriminals intent on breaching your network to access customer and financial data.
- Nation-states motivated by political and ideological differences.
- Hactivists and cyber-terrorists seeking vulnerabilities in the network to disrupt government business.
- Insiders able to inflict twice as much damage because of proximity and access to systems.

Any of these bad actors can be motivated by money, politics, and perceptions far too numerous to detail here.

> **New bots are continually evolving to be smaller, harder to detect, more effective and more organized, making them impossible to flush out of systems.**

Known methods of attack

It's impossible to describe all the methods that may be used to launch an attack on your organization, because the scope is expanding all the time. Some of the more prevalent methods are worth understanding:

Social engineering: Your own employees can unwittingly become conduits of attack. From public websites that target your enterprise to well-crafted spear phishing emails, bad actors can hook even senior and savvy employees. New bots are continually evolving to be smaller, harder to detect, more effective and more organized, making them impossible to flush out of systems.

Distributed Denial of Service (DDoS): DDoS attacks and 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.

Ransomware: Infected networks and systems allow criminals to encrypt data and resources to hold them hostage until some form of payment is made. City governments, municipal hospitals and others who touch the public have proven to be quite susceptible. This attack has become so prevalent that there are now criminal networks offering "Ransomware as a Service" operations whereby they provide the technology to a would-be less-sophisticated attacker for a cut of the ransom.

Supply chain exploits: Modern systems are often composed of numerous pieces of software working together. Sometimes, a piece of software from one vendor contains software from a third party that fills some niche but important function in the larger program. If that component part is less secure it provides an entry point into the larger system. The 2020 SolarWinds attack, for example, was based on a software component compromised by nation-state-sponsored bad actors who inserted a "backdoor" access point into its code. As that code became incorporated into software from other vendors, that backdoor was replicated in these other programs with thousands of ultimate customers affected.

The threat landscape

This overview of the threats mentioned above and the types of attacks included in this brief are just a snapshot in time of the constantly evolving landscape. Securing a government-related financial institution's computing and network resources must evolve as well, taking a holistic approach.

Fortunately, these institutions can turn to a broad technology industry for security innovations. Yet, even this obvious strategy is not as simple as it once was when discrete technologies defended against specific forms of attack. Modern security strategies are built on flexible, integrated security frameworks that incorporate discrete technologies into a proactive security posture.

Choosing the right industry partner

Lumen has a long history of protecting the financial services industry and government agencies from attack. Connected security is a key pillar in the Lumen platform along with adaptive networking, edge cloud and collaboration services. This intersection of platform and security enables Lumen to take a holistic view of security.

It starts with the network where core security comes built in. Specific services can be layered on top of that network, tailored to a customer's unique needs. Lumen integrates these additional services and technologies so the customer can deal with one provider for support, billing and the peace of mind that someone is accountable for the solution.

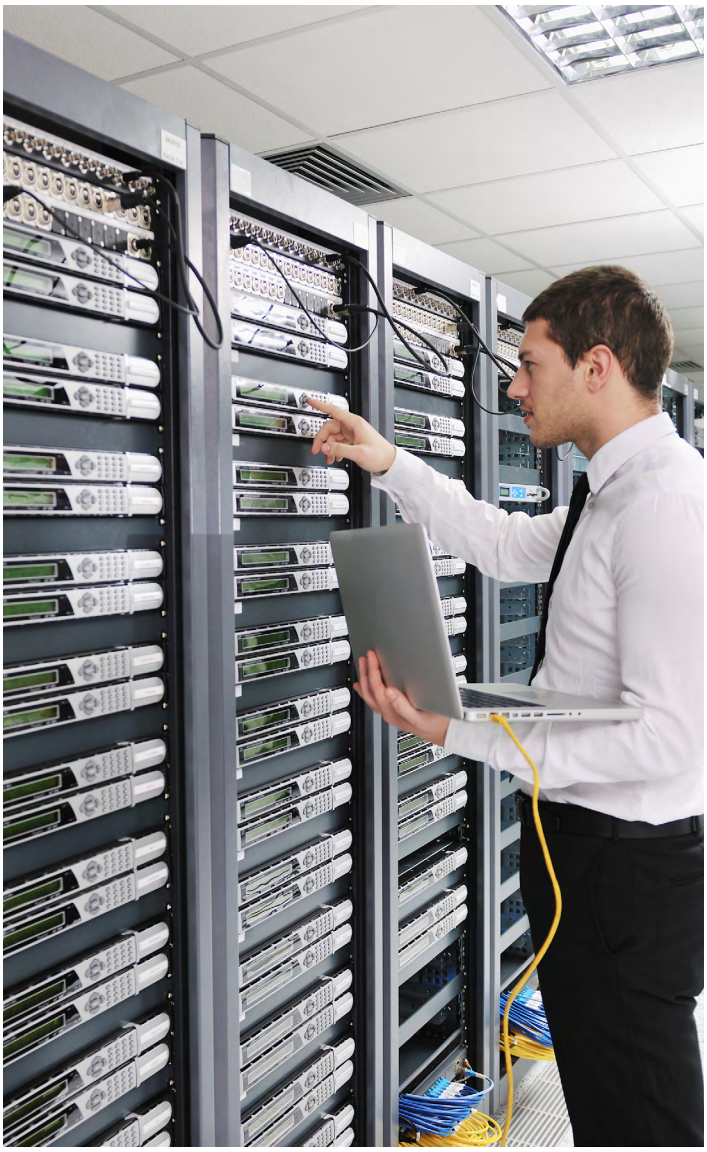
Lumen's platform approach also allows the company to work with an ecosystem of technology companies to select best-of-breed services to fill key roles in that holistic framework. That platform and ecosystem model is key for delivering modern security toolsets such as Zero Trust and Secure Access Services Edge (SASE), both of which are concepts that require multiple integrated technologies. Lumen works closely with these providers of software and other technologies so they are integrated with the platform and Lumen engineers become experts in those components. This platform and ecosystem approach also enables a flexible, evolving security posture as new threat types emerge.

Holistic security is more than technology per se. You need to have visibility across your enterprise to truly understand what's happening and proactively defend against threats. Lumen is a primary carrier on the internet backbone, providing Black Lotus Labs, Lumen's threat intelligence unit, unparalleled access to deploy sophisticated threat-sensing analytics on the Internet backbone. This is coupled with machine-learning engines to classify potential threats such as botnets and malicious entities of various types and locations. With Black Lotus Labs, Lumen can identify threat patterns before customers experience an impact. Countermeasures can be automatically triggered to head off or mitigate attacks.

Security Operations Centers (SOC) are another important part of a proactive, holistic approach to security. SOCs are the hubs where security experts command the security technologies, analyze data and manage the agency's security posture. However, staffing these centers and ensuring you have the right solutions deployed can be challenging.

The SOC can be offered as a service – SOCaaS. Lumen operates state of the art SOCs, designed for government agency needs and with the ability to support federal mandates such as the move to Zero Trust through managed security services. Agencies don't need to worry about finding talent or investing to maintain state-of-the-art technologies in their SOCs. They also cannot replicate the capabilities already present in Black Lotus Labs, which stands behind all Lumen SOCs.

Because Lumen has a long history of supporting both the finance industry and government, it understands demands from both sectors. This can be a great benefit for these institutions that straddle the line between commercial and governmental roles. Some buy from commercial enterprise contracts and some buy via federal contracts. Lumen can handle both.



Conclusion

In the past, cybersecurity was based on a castle and moat approach. Specific technologies such as firewalls provided the moat protecting the castle and there were certain protocols in place whereby the metaphorical drawbridge could be lowered. That approach is no longer sufficient for what has become an arm's race between bad actors and those with assets to protect.

The unique set of institutions at issue in this paper, with financial responsibilities including regulation and enablement, provide a tempting target for a small army of bad actors, their greed or grievances and their arsenal of hacking tools. Real security starts with a mindset and a strategy before layering in technology defenses. Defense alone is not enough, and Lumen brings resources such as our cyber-intelligence arm, Black Lotus Labs so cybersecurity can act with a proactive edge.

Today, you need a comprehensive plan that keeps you ahead of the bad guys. Contact your Lumen public sector representative to secure your institution.

888-597-2455 | lumen.com/public-sector/solutions/security