With great growth comes great data responsibility

Fintech firms must safeguard a prized asset—customer financial data. To keep data out of the reach of cybergangs targeting the sector, fintechs must embrace cyber hygiene.

Key takeaways

- With cybercrime skyrocketing, consumer-facing outfits like fintechs are adding greater layers of security.
- To define their attack surface, fintechs must know their endpoint totals, configuration, software and patches.
- Good cyber hygiene and "shift left" software testing usually send criminals in search of easier prey.

> With fintechs, data is the product. If portfolios are stolen, that is a huge damage to reputation.

Tim Morris
Former SVP of information security,
Wells Fargo

As senior vice president of information security at **Wells Fargo**, Tim Morris relished the 48-hour cyberattack simulations the bank held in local auditoriums for its massive security teams.

"We'd have about 100 people, from all the security divisions," says Morris of the marathon sessions where he oversaw simulated red-team offensive assaults ranging from simple email phishing campaigns to sophisticated ransomware attacks. "We did every kind of security incident and attack you can imagine, from distributed denial of service to large-scale data exfiltration attempts." He laughs: "After two days, people would be pretty tired."

For decades, and even centuries, banks and insurers have been the gatekeepers of sensitive customer financial information. Now, in the age of **financial technology** (a.k.a. "fintech"), that data is almost exclusively digitized—from paycheck deposits and mortgage payments to mobile trading platforms and Bitcoin holdings. The business stakes are much higher, too.

"With fintechs," says Morris, "data is the product. It is the livelihood of their customers. If deposits or portfolios are stolen, that is a huge damage to reputation."

Thanks to technology and pandemic-induced remote working, fintech networks are now baked into nearly every consumer, e-commerce, and investor transaction. Whether you're a fan or a skeptic of fintech, it is set to get bigger, much bigger. The sector's global e-commerce volume will be $3.61 trillion this year, up from $348.7 billion in 2010, and is estimated to reach $6.07 trillion in just five years, according to Ascential's Money20/20 report.

The cybersecurity threat will rise as well. Consistently, among all industries, banking has borne the brunt of cybercrime costs. In 2019, it came in a dismal No. 1 in Accenture's Ninth Annual Cost of Cybercrime study. Things have only gotten worse since then, as the global cost of all cybercrime skyrocketed to nearly $1 trillion in 2020, thanks to the pandemic and remote work. Last year's cyberattack on the digital banking app Dave, in which hackers stole the personal data of about 7.5 million dave.com users, shows the vulnerabilities the fintech sector faces.

To many critics, the algorithms that support online payment, insurance, and lending platforms are a key issue in their stability and reliability. That's not actually the case, says Morris. What's truly critical is how these companies manage data and the robustness of the systems that secure it.

Tanium's Cyber Hygiene Assessment: An actionable path to better endpoint management and security →

$3.61 trillion

The fintech sector's global e-commerce volume this year, which is expected to nearly double by 2026

Crown jewels

Moshe Katri is managing director of equity research at **Wedbush Securities**, a wealth management and investment firm with some 6,000 clients and $4.2 billion under management. Katri says that just because fintechs are innovative, it doesn't mean they're taking higher risks.

In fact, consumer-facing businesses like fintechs that are operating in fields with greater volatility, be they crypto exchanges or share-trading platforms, tend to add layers of security. "The last thing they want is to have confidence shaken with a breach," says Katri

Not surprisingly, Morris, who now works as a technology strategist at **Tanium** in North Carolina, says visibility across the entire network is key to data security. To achieve that, fintech players need to know **how many endpoints** are on their network, how those **endpoints are configured**, what **software they are running**, and whether that software is patched and up-to-date. Only then can they define their attack surface and secure their crown jewels. Stepping back a little, he says, fintech firms should also have a grasp on what they themselves look like to an attacker.

Own it

Cybercriminals **target the fintech sector** for the same reason they target others, for a quick payday (often through ransomware). That gives security firms something to work with and anticipate. Also, according to Morris, while attacks often look increasingly sophisticated, they are usually opportunistic and well planned. Ransomware, he says, is becoming "commoditized."

Deploying good cyber hygiene practices is key to making it harder for criminals to break in, which is often enough to send them looking for a more vulnerable victim. Among the best: finding and inventorying all the endpoints and devices connected to a network; managing the growing number of apps and other software that have proliferated during the remote-work era; automating the patching of sanctioned software (while getting rid of rogue apps); and creating a rapid-response plan to security threats.

Morris says that fintech firms must embed security early into their operational technology, a practice known as "shift left" software testing. This prioritizes testing earlier in the development cycle, rather than bolting it on after the fact. It also encourages, if not requires, more collaboration between security teams and developers.

> **Firms should have a grasp on what they themselves look like to an attacker.**

[Read also: Measuring what matters: aligning risk measurement with corporate goals and objectives]

"I often use a house as an analogy," says Morris. "You figure out the boundaries and the locks as you are configuring the windows and the doors."

A challenge for the fintech sector, populated as it is with many small companies, is the temptation for businesses to outsource all responsibility for their IT and security. Fintechs can't simply rely on a vendor for every need. (Recent supply chain attacks have surely taught them that.) They can't set it and forget it. They need to own their security strategy. Putting it at arm's length creates a third-party risk for the company in addition to data risk, says Morris.

It also runs afoul of regulators. A fintech's information system must not only meet its own business requirements but also those of financial **and security regulators**. They must also meet the protocols of financial services partners or sponsors. And they can't be off-the-shelf.

"You need really good rules, not canned or templated rules,'' says Chuck Pine, who heads the compliance practice at accounting and advisory firm **BDO**, and whose team focuses on anti-fraud and anti-money laundering strategies. "They need to be built for your customers or your clients."

Evolving threats

In an environment where digital transformation continues to quicken, digital threats are also rapidly evolving. That makes fintechs one of the most important guardians of prized customer data and underscores the importance of the sector to maintain tough cyber hygiene practices.

Pine says companies starting out in the fintech space and embarking on compliance often don't understand that their risk profile is inherently high because of the nature of the businesses they are operating in.

[Read also: Europe's hefty regulatory fines are roaring back]

Fintech itself is also a changing landscape. Crypto, which seems to **steal the headlines**, is an innovation that offers investors a product, digital coins, and a new technology, the **blockchain**, which in theory has the potential to change the entire plumbing of the financial services industry. The platform's proponents say its encrypted transactions take financial services security to a new level, while critics say it's open to abuse because of settlement anonymity.

Katri at Wedbush says a lot of energy at crypto ventures is going into anticipating the potential introduction of regulations, or at least more oversight.

"Crypto will get regulated one way or another," says Katri. "It will be a positive event for the industry and provide some legitimacy."

Back to basics

Data isn't just a prized asset for fintech firms. It can drive technological innovation and open up new markets. Get it right and fintechs stand a strong chance of thriving. But if there are stumbles, system failures, or breaches, there will be pressure on U.S. watchdogs to crack down and impose parameters that may threaten the growth that has carried the sector to where it is today.

[Read also: Laternal movement: how cybercriminals move across your network and how to stop them]

For Morris, a lot of it comes down to good old-fashioned cybersecurity practices. When you're carrying out threat assessment and you see a potential pathway for an attacker to get into the system, "you feel a pit in your stomach," he says. "But you also feel good because you have found something before anybody else."