INSIDER INTELLIGENCE | eMarketer

MAY 03
Sherry Fairchok

Spike in destructive attacks, ransomware boosts banks' cybersecurity spending in 2022

Article

The news: Banks are **doubling down on their security budgets this year** to protect against a spike in **destructive attacks, ransomware, and "island hopping"**—a term describing the process of undermining a company's cyber defenses by going after its vulnerable partner network, rather than by launching a direct attack.

That's according to cloud computing and software provider **VMware's** report, "Modern Bank Heists 5.0."

- Its findings are based on a February 2022 survey of 130 chief information security officers and security leaders at financial institutions, 41% of which were headquartered in North America.

By the numbers: The majority of financial institutions surveyed plan to increase their security budget this year.

- Seven out of 10 financial institutions that VMware interviewed aren't spending more than 12% of the overall IT budget on security. But the **majority of financial institutions plan to increase their budget by 20% to 30% this year**.
- IBM's most recent report on cyber attacks found that the financial industry is already spending the second-most of any industry fighting off attacks, with **an average cost of $5.72 million per data breach**.
- Just a few years ago, Accenture found financial services to be **the most expensive industry from which to fight attacks**. For example, **Bank of America's** CEO Brian Moynihan said it spends over $1 billion yearly on cybersecurity.

Destructive attacks: The VMware report indicates that **63% of financial institutions experienced an increase in destructive attacks**, an increase of 17% from last year.

- Destructive attacks are launched punitively to destroy data and dismantle subnets. Typically, cybercriminals leverage these attacks as an escalation to destroy the evidence as part of a counter-incident response.
- Destructive malware variants seek to destroy, disrupt or degrade victim systems by encrypting files, deleting data, destroying hard drives, terminating connections, or executing malicious code.
- In the financial industry, companies **reported 703 cyber attack attempts per week in Q4 2021,** a 53% increase over the same period in the previous year, per Banking Journal. Some studies

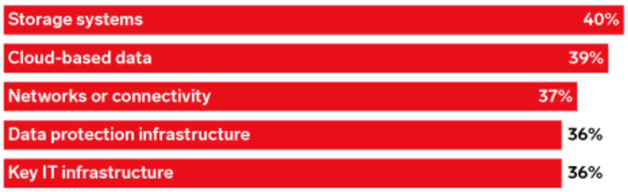
estimate that, on a global scale, the rate of cyber attacks is one every 10 seconds.

Ransomware: In addition, **74% of respondents experienced one or more ransomware attacks**, and 63% of those victims paid the ransom.

- Uses remote access trojans (RATs) that help cybercriminals gain control of systems.
- Attackers can choose from an array of readymade and available ransomware kits—for example, from **Conti,** a ransomware group known for its ransomware-as-a-service (RaaS) structure. Cybercriminals use the kit to compromise a network, encrypt sensitive files within the network, and send the victim a ransom note that asks for crypto in exchange for a decryption key that will unlock access to the files.
- The cryptocurrency investigation and compliance solutions provider **Chainalysis** corroborates this finding: It's identified **more than $602 million worth of ransomware payments paid in 2021**—with the Conti ransomware gang accounting for $180 million—although it says the true total for 2021 is likely to be much higher.
- In a six-month span last year, the financial crimes investigation unit of the US Treasury Department (FinCEN) said **it identified approximately $5.2 billion in outgoing bitcoin transactions potentially tied to ransomware payments**.
- Governments are now persecuting crypto exchanges that facilitate financial transactions for ransomware attackers; for example, the US Department of the Treasury Office of Foreign Assets Control's (OFAC's) issued sanctions against the Suex cryptocurrency exchange in September 2021.

Areas of Enterprise IT Environment Affected by Successful Ransomware Attacks According to IT and Cybersecurity Experts in North America and Western Europe, Jan 2022

% of respondents



Source: OwnBackup, "The Long Road Ahead to Ransomware Preparedness" conducted by Enterprise Strategy Group, March 31, 2022

274552 eMarketer | InsiderIntelligence.com

Island-hopping: And **60% of financial institutions experienced an increase in island-hopping**, a 58% increase from last year.

- VMware said that "mere wire transfer fraud is no longer the ultimate goal"—instead, it's "hijacking the digital transformation of a financial institution to attack its constituents."
- The firm's Threat Analysis Unit said it's found that cybercrime cartels have **studied the interdependencies of financial institutions** and understand which managed service providers they use and who their outside general counsel is. T**hey target these organizations and hack them to island hop into the bank**.
- 87% of financial institutions are concerned about **cyber defenses used by their shared service providers**. If these firm's infrastructure is compromised, it can pose a systemic risk to the financial sector as malefactors can attack dozens of financial institutions at a time.
- 94% of financial security leaders experienced **attacks on an API associated with fintech**. VMware describes APIs as "essentially the central nervous system" carrying data between applications. Consequently, they make "a perfect target" for cybercrime cartels, particularly because they're designed to be highly accessible.

What should banks do? Cybersecurity is a brand protection imperative. Consumers' trust and confidence in banks' stewardship of their assets depends on their effectively avoiding, mitigating, and responding to cyberthreats.

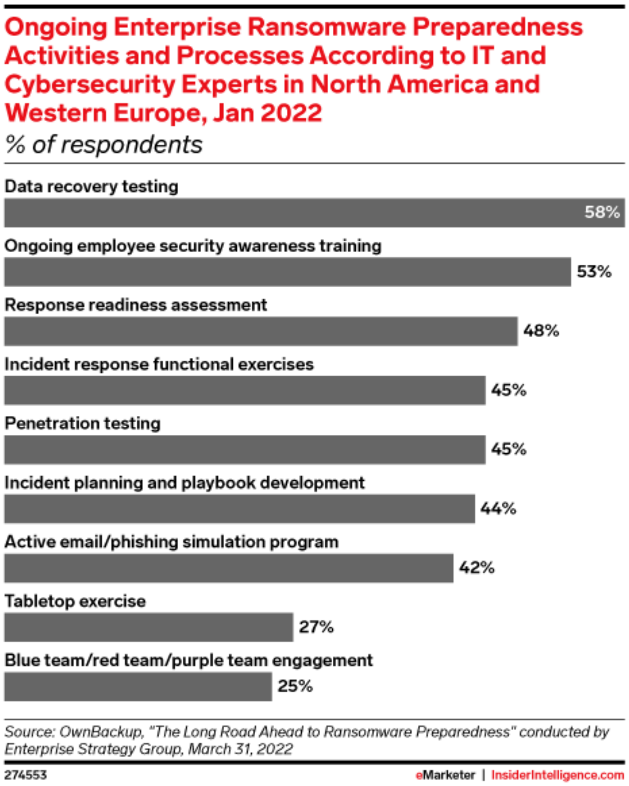
Under new reporting requirements, which went into effect on May 1, financial institutions **must immediately notify law enforcement if they suspect a ransomware transaction has taken or is taking place**.

- President Biden's signing of the Cyber Incident Reporting Act requires owners and operators of critical infrastructure to report cyber incidents to the U.S. Department of Homeland Security (DHS) and CISA within 72 hours and ransomware payments within 24 hours.

VMware further recommends that instead of trusting in the strength of their incident response, security teams should **adopt threat-hunting on a weekly basis**—to be more proactive in safeguarding their systems.

- Threat-hunting focuses on the pursuit of attacks and the evidence attackers leave behind.
- It also gathers intelligence, which has even more value to a cooperative industrywide effort—for example, when collected by the Financial Services Information Sharing and Analysis

Center (FS-ISAC).



Ongoing Enterprise Ransomware Preparedness Activities and Processes According to IT and Cybersecurity Experts in North America and Western Europe, Jan 2022

% of respondents

Source: OwnBackup, "The Long Road Ahead to Ransomware Preparedness" conducted by Enterprise Strategy Group, March 31, 2022

274553 eMarketer | InsiderIntelligence.com