5 CRITICAL CYBERSECURITY ACTIONS FOR THE FINANCE INDUSTRY IN 2024

digicert®

Every year, the Financial Services Information Sharing and Analysis Center (FS-ISAC) gathers for the FinCyber Today Summit. Here, the world's leading cybersecurity minds in the financial sector collaborate to build a strategy against cybercrime and digital attacks that threaten consumers, financial institutions, and the global financial infrastructure. This is what the brightest financial cyber experts see coming in the next year—and what you should do to protect your organization and clients.

THREATS ON THE RISE

300X

More likely attackers target finance over other industries

63%

Increase in the number of finance industry cyberattacks 2021-2022

47%

Of businesses expect customers to switch institutions after a breach

1. INVEST IN VALIDATION TO GUARD AGAINST CHANGES IN THE LANDSCAPE—LIKE AI

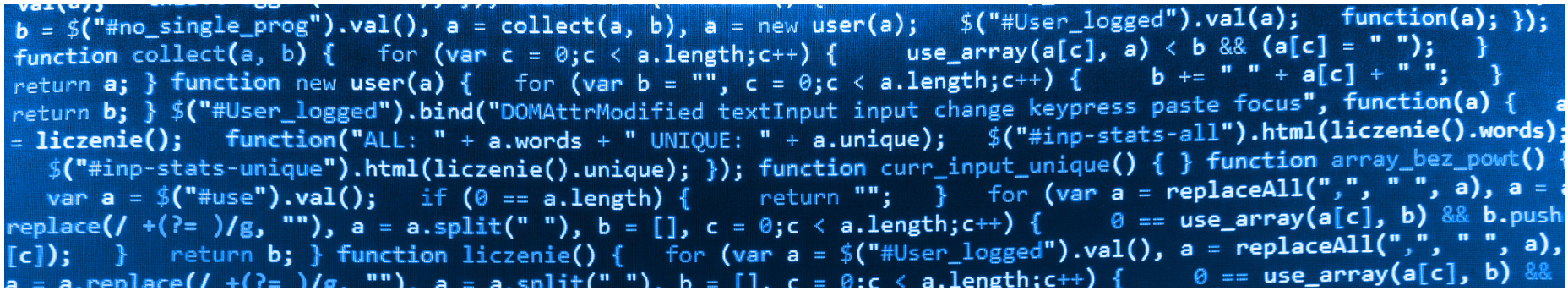
Recent advancements in technology make it easier for criminals to develop sophisticated attacks with very little effort. The most obvious concern is artificial intelligence, which helps attackers mimic bank employees or customers and their families, crafting convincing phishing emails on a large scale in a variety of languages. These AI-constructed emails have far fewer grammatical errors than other phishing scams, making them more difficult to catch.

In response, email providers and financial security experts recommend investing in authentication protocols like DKIM, SPF, DMARC, and Verified Mark Certificates (VMC). Email validation is increasingly important, and while it's becoming easier to create convincing content, domain validation isn't easy to spoof. Digital signing of email with S/MIME is also a defense against phishing and social engineering.

2. DEPLOY SIGNING, SCANNING, AND SBOMS TO MANAGE RISKY LINKS IN THE SOFTWARE SUPPLY

Software supply chain attacks continue to increase, with many devastating breaches in recent years. These attacks can affect hundreds of thousands or millions of clients and users, and they can cost institutions millions in remediation and damage to a brand's reputation. Today, software is built on components gathered from across the software supply chain, with code deriving from third parties, runtime, SDKs, libraries, and other dev teams inside and outside organizations. Cybercriminals frequently make use of the obscurity involved in this conglomeration of components to hide breach points and malware inside software builds.

Increasingly, cybersecurity experts point to a Software Bill of Material (SBOM) as a highly effective defense against the kind of obscurity cybercriminals rely on to embed attack vectors into code. An SBOM, like a list of ingredients on a food package, is a complete inventory of all the components in the build. It helps security teams understand where each software component originated and whether or not it can be trusted. In conjunction with scanning, code signing, and other best practices, an SBOM helps institutions detect and eliminate threats before they lead to costly breaches



3. ENSURE YOUR DIGITAL SECURITY MEASURES MEET BUSINESS AND LEGAL COMPLIANCE

Despite the fact that the number of PKI certificates continues to grow exponentially—even within organizations—many companies still manage certificates manually. Expired certificates are a significant source of exposure to criminals, and many institutions aren't aware of the number or types of certificates on their network. An expired certificate on something as benign as a smart refrigerator in the break room can give an attacker access to an institution's network and systems. In an effort to make certificate management less fraught, Google continues to push for shorter expiration periods on web certificates. But that doesn't address devices, users, email, and other potential entry points.

Automated certificate lifecycle management is the new industry standard for protecting entire organizations. Today's managers can detect and inventory all certificates inside an ecosystem, no matter what that certificate is attached to. Once inventoried, automated processes renew or replace expiring certificates and warn of outages for quick responses. This helps financial institutions make sure they don't have any hidden entry points and discover and fix lapses before someone can steal data.

40% – 80%

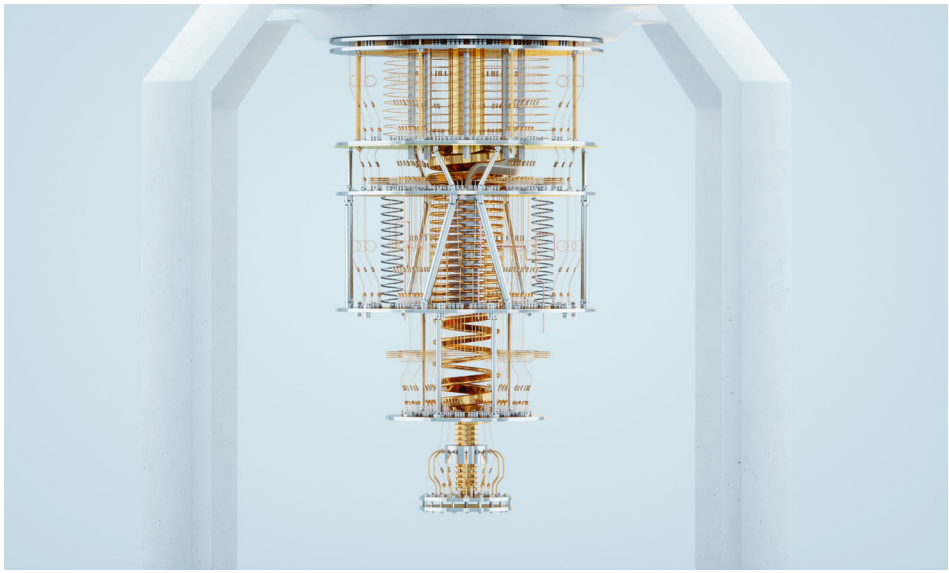
Of lines of code in most new software derived from 3rd-party vendors*

Gartner study

4. BEGIN PREPARING FOR POST-QUANTUM CRYPTOGRAPHY—IMMEDIATELY

Like AI, quantum computing will be here faster than you might expect. For decades, the backbone of digital financial transactions and security has been cryptographic algorithms that quantum computers can easily break. While quantum computing offers some great advantages to the financial industry, it also has the potential to fully eliminate the safeguards that protect assets, institutions, and clients.

In anticipation of this technological revolution, cybersecurity experts are developing quantum-resistant solutions. Known as Post-Quantum Cryptography (PQC), these new algorithms are difficult for quantum computers to analyze and crack. Financial institutions should be deploying PQC solutions immediately to combat the very real concern that attackers will employ a "harvest now, decrypt later" strategy, holding onto stolen and encrypted data until they can gain access to quantum for decryption in the near future.



5. SECURE ONBOARDING OF NEW CUSTOMERS WITH STRONG IAM

Financial institutions are still working through rapid changes prompted by the COVID-19 pandemic. One of those rapid changes involves different methods for opening new accounts. Today, institutions need to be able to create accounts remotely and securely. They also need to be able to validate identities without sitting down in-person with a new client who can show verified forms of ID. High-assurance identity verification, conducted remotely, is a critical need for financial institutions.

These institutions should look to Remote Identity Validation (RIV) and other forms of identity and authentication tools that embed cryptographically unique verification to digital IDs. The very nature of the cryptographic identity makes these forms of digital validation extremely difficult to fake, and in many cases, they are more secure than traditional forms of identification. In many countries around the world, cryptographically secured digital identity is recognized as legal identification, equal or superior to ID cards and passports. This trend toward digital identity is likely to increase, and these forms of validation can help financial institutions protect themselves and their clients as they continue to transact through the internet and apps.

ABOUT DIGICERT

Digital trust has become the backbone for security in the connected world. DigiCert is the leading provider of digital trust, enabling companies and individuals around the globe to navigate the connected world with the confidence that their digital footprint is secure.

To learn more about digital trust for financial institutions, visit us at https://www.digicert.com/campaigns/banking-security-and-digital-trust

digicert®