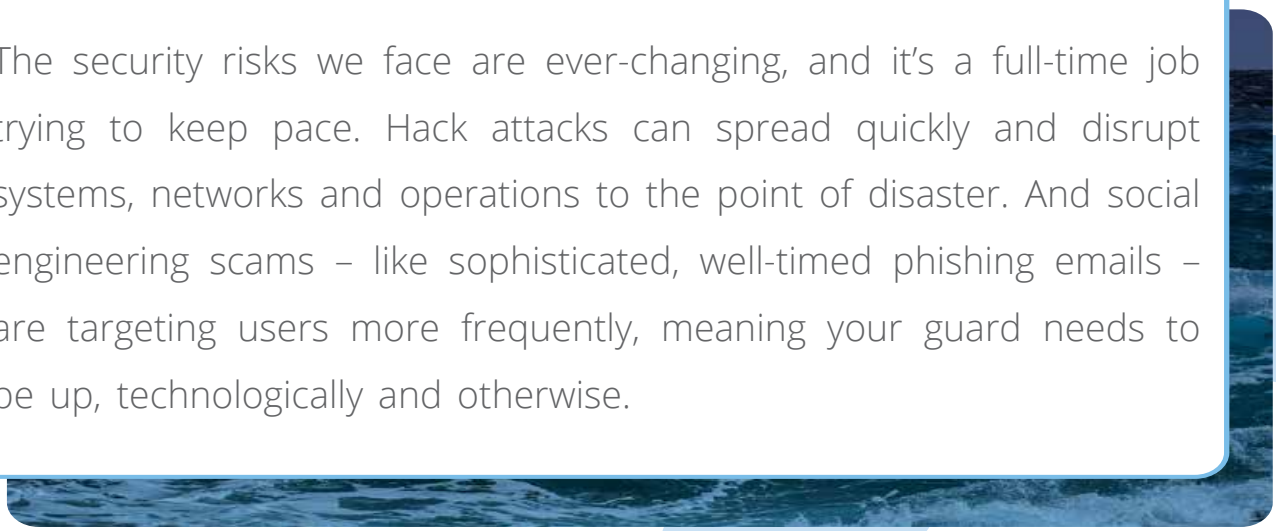
BluWave

10 Common Cybersecurity Gaps

AND HOW TO AVOID THEM

BluWave

The security risks we face are ever-changing, and it's a full-time job trying to keep pace. Hack attacks can spread quickly and disrupt systems, networks and operations to the point of disaster. And social engineering scams – like sophisticated, well-timed phishing emails – are targeting users more frequently, meaning your guard needs to be up, technologically and otherwise.



Unfortunately, many firms often fall short when it comes to their cybersecurity protections – and they don't often realize it until it's too late. Our hope in sharing these 10 IT security gaps is to highlights areas where financial services organizations can take steps now to avoid risk in the future. These gaps are preventable, and when the next phishing email hits your inbox or ransomware attack strikes your network, you can rest easier knowing you've plugged these common security gaps.

Here are your 10 Common Cybersecurity Gaps (keep reading for tips on how to avoid them).

1. Risk Management and Governance
2. IT Asset Management
3. Vulnerability Assessments (and Penetration Tests)
4. Patch Management
5. Social Engineering & User Training
6. Business Continuity Planning
7. Multi-factor Authentication
8. Third Party Vendor Management
9. User Provisioning and Management
10. Incident Response Planning/ Procedures

The Risk Assessment

Before we jump into the 10 common gaps, let's first address the activity that often identifies these cracks in security: the risk assessment.

WHAT IS A RISK ASSESSMENT?

Generally, a risk assessment is the process of identifying risks and exposures present across a particular program as well as evaluating the potential impact of those risks. More specifically, according to the National Institute for Standards and Technology (NIST), the goal of the risk assessment is to understand, "the cybersecurity risk to organizational operations (including mission, functions, image or reputation), organization assets, and individuals."

Some questions that should be asked during the risk assessment process include:

- What are the most critical cybersecurity threats (internal and external) to your business?
- How are you protecting against those threats?
- What assets, systems, and technologies do you have in place?
- Who maintains ownership of those assets, systems, and technologies?

Once these questions have been addressed, it's time to find out if your bases are covered. Following are 10 areas where firms often miss the mark.

1. Risk Management and Governance

Kicking off our Top 10 Gaps, it seemed wise to start with the one that sets the tone for the organization's cyber strategy. Ultimately, what this gap highlights is the need for financial services organizations to employ official governance policies around cyber risk management.

WHO OWNS THE RISK AT YOUR BUSINESS?

Cyber strategy and programs start at the top, so your leadership team/executive board should be involved in discussions around cybersecurity preparedness. You should also designate a Chief Information Security Officer (CISO) to oversee the firm's security posture. Oftentimes, this individual holds a dual-role within the firm, also operating as the Chief Compliance Officer or Chief Technology Officer.

Risk management does not end with the CISO, however. In fact, he/she is only the beginning. There should be broad support and input across the firm with regard to cybersecurity practices and governance policies. Once these questions have been addressed, it's time to find out if your bases are covered. Following are 10 areas where firms often miss the mark.

Depending on the size of your firm, this group may be large or small, but should include individuals responsible for operating the controls in place to secure the business. In addition to contributing to and managing the proactive security
functions of the firm, this group (or a portion of it) may also take the form of a Computer Security Incident Response Team (CSIRT).

Outsourcing is extremely beneficial from a day-to-day cyber risk management perspective, but the accountability and responsibility for the firm's security posture lies with the firm itself.

PRO TIP

If you leverage managed service providers for all or part of your firm's security program, it's important to have thorough and comprehensive documentation in place to address that relationship. At the end of the day, risk management and governance fall solely on you, as your organization is the one who answers to investors, regulators, etc.

IT Asset Management

2. This critical security gap occurs when financial firms fail to maintain a complete inventory of their technology assets. This includes keeping a running list of: workstations, servers, applications, and smartphone devices such as phones, tablets, laptops, and more. Now more than ever, with many firms adapting a hybrid work model, it is important to understand your inventory.

Often forgotten on this list are other devices that store information (phones, printers/copiers, etc.) as well as the growing collection of Internet of Things (IoT) systems including conference call equipment, wireless speaker systems, and the like. Anything connected to your firm's network should be inventoried and cataloged.

Why, you ask? Because you can't properly assess your firm's level of risk or adequately protect data and information unless you understand what systems you have and what data they hold.

Also, as your firm grows in assets, products, and headcount, are you remembering to re-evaluate your IT inventory? At the bare minimum, firms should conduct an annual review cycle of all IT assets to understand if there have been additions, deletions or changes in how that technology is managing data and what controls are in place to protect it.

PRO TIP

Don't forget to include third party vendors in your IT asset management. Do you maintain a log of what service providers you work with and who has access to what information? If not, start now.

3. Vulnerability Assessments and Penetration Tests

In order to construct the right defenses, firms must have a clear understanding of their IT security vulnerabilities. Through regular vulnerability assessments and penetration tests, firms can identify real and potential risks that exist internal and external to the network – a critical first step to resolving and remediating threats.

VULNERABILITY ASSESSMENTS VS. PENETRATION TESTS

The vulnerability assessment (VA) scans networks to determine areas of vulnerability and creates a database on known risks, often classified based on their unique severity. Picture a dot in the middle of a circle scanning from the inside out.

Penetration testing, in contrast, uses testing tools to simulate real-world attacks and determine if a would-be hacker could gain entrance into the firm's network. In our circle example, the dot is on the outside trying to break through the barrier.

The key to VAs and pen tests is taking a risk-based approach, which oftentimes financial firms fail to do. Having hopefully identified key risks during the risk assessment process, firms should use those risks to tailor their approach to vulnerability assessments and ensure they scan for critical threats.

PRO TIP

If you leverage managed service providers for all or part of your firm's security program, it's important to have thorough and comprehensive documentation in place to address that relationship. At the end of the day, risk management and governance fall solely on you, as your organization is the one who answers to investors, regulators, etc.

4. Patch Management

Patch management is becoming a top-tier question on investor due diligence questionnaires (DDQs) as they look for reassurance that financial firms are staying current with software and system upgrades.

The key to successful patch management is applying patches appropriately – and as quickly as possible. Some systems have regimented processes that roll out updates automatically, but others are not as disciplined and require diligence on the part of systems administrators/IT teams to stay current.

Of particular concern are zero-day threats – attacks that take advantage of software vulnerabilities before patches and updates are available to the public. These exploits are obviously difficult to protect against, but the most effective method of protection is to install updates as soon as they become available. Having a patch management process in place in advance will allow firms to roll out updates efficiently and quickly, when necessary.

PRO TIP

Automate patches (when possible). This will ensure you stay on top of security patches as they roll out and reduce the likelihood of glitches, zero-day attacks or malware threats. Remind users to save their work, but leave their computers ON, as most patches will require a reboot to ensure applications are not running in the background (this can make patching tricky and ineffective).

5. Social Engineering & User Training

According to the 2021 Verizon Data Breach Investigations Report:

- Financially Motivated Social Engineering is increasing year over year.
- Business Email Compromises are the second most common form of Social attacks.
- Hackers continue to evolve their tactics - misrepresentation is 15 times higher than last year.
- The good news: increased awareness and employee phishing and social engineering training is working. The click rate in phishing simulations is down to a median of 3%.

The ultimate goal of social engineering is to trick users into divulging information (credentials, personal financial information, company financial information, etc.), and the results have been staggering. Corporate account takeover scenarios and business email compromise (by way of phishing scams) are becoming incredibly successful as they increase in sophistication and users struggle to keep up with hard-to-recognize hacker tricks.

PRO TIP

The key to mitigating social engineering scams is awareness. Awareness of these common tricks will alert users to their typical maneuvers and keep them on their toes as fresh emails hit their inboxes and social media alerts pop up on their mobile devices.

Phish your own employees.

Business Continuity Planning

6.

Business continuity planning (BCP) seems like a no-brainer in this day and age, but unfortunately, many firms still miss the mark as it relates to their security posture and preparedness. Some BCP gaps commonly identified during the risk assessment process:

- No business continuity or recovery plan in place
- BCP hasn't been updated within a year
- Plan does not take a risk-based approach or deal with specific risk scenarios unique to the firm
- A plan exists on paper, but employees have not been educated or trained on it

The above examples highlight critical gaps in business operations that could lead to significant repercussions in the event of a security incident. Beyond dealing with the technical aftermath of a cyber-breach, financial firms must have continuity plans documented for the recovery of the business operations – including communication to internal and external parties, employee roles and responsibilities, and prioritization of business functions.

PRO TIP

Conduct annual tabletop and simulation exercises to ensure employees are effectively trained. These can be in-person or virtual seminars but should bring together department representatives across the firm to enable swift business recovery in the event of a business-impact scenario.

7. Multi-Factor Authentication

Hackers have become savvier over time, and strong passwords are no longer solely effective in thwarting their sophisticated attacks. With the use of two-factor or multi-factor authentication, however, users can add an additional layer of complexity to their security practices and make it more challenging for hackers to exploit gaps.

Multi-factor authentication (MFA) should be enabled on all devices and applications that allow it, including cloud platforms and remote access gateways (e.g. Citrix), social media sites, and web-based applications.

Commonly used authentication factors include:

- Knowledge-based (e.g. security questions)
- Possession-based (e.g. RSA token, one-time code sent via SMS)
- Inherence-based (e.g. biometric scan, fingerprint)

Multi-factor authentication is gaining wide popularity as a simple, yet effective way to add an additional layer of security to users' behavior. If there's a complaint, it may be that it takes a few extra seconds to log into systems, but most firms prefer such a trade-off between security and convenience. they increase in sophistication and users struggle to keep up with hard-to-recognize hacker tricks.

PRO TIP

In order for multi-factor authentication to work effectively, it's critical that firms avoid using shared logins across their systems and applications. Shared user IDs and accounts leave the door open for a security incident – whether internal or external in nature.

8. Third Party Vendor Management

Arguably the most concerning and risk-infused of these security gaps is the risk inherent in employing third party vendor relationships. Even if your firm has employed all of the security features and best practices we've highlighted thus far, do you feel confident your outsourced service providers have done the same?

Managing vendor risk is a full-time job, and unfortunately, many financial firms still fall short in this regard. A few critical questions to ask:

- Have your managed service providers shared copies of their DR/BCP reports, vulnerability assessment reports, SOC audits, and data center facility certifications?
- Do your third party providers keep an inventory of their systems, data and applications? (Remember #2 – IT Asset Management?)
- How do your vendors manage their vendors (e.g. contractors, data center providers, external security providers, etc.)?

These and many other questions should be asked during a thorough and annual due diligence process with all third party service providers. In addition to understanding your firm's own risk, it's equally as important to understand the risks and exposures present as a result of your outsourcing partners.

PRO TIP

One often overlooked contributor to service provider risk is contract termination. Financial firms should be careful to thoroughly read and review contracts with third-party providers and vendors and have a clear understanding of the termination process. Risks may vary depending on the level of access the service provider has to your firm's data. Be sure to look for any contractual loopholes and operational practices that may affect migration plans or your firm's security standing.

9. User Provisioning and Management

Paramount to warding off malicious and unintentional security threats is access control. And whether your financial firm has 20 users or 200, it requires detailed and stringent access control policies to ensure data and sensitive information is restricted to only those who need it.

Some firms leverage user provisioning software to facilitate the process of provisioning new users and managing access, but many firms are still doing things the old-fashioned way. Truthfully, the old fashioned way can be effective – as long as the firm and its IT administrators understand and employ the principle of least privilege. This principle states that access should be limited and based strictly on those who need it. Using varying levels of access or individual user account specifications allows firms to better safeguard confidential information regarding company financials, investor information, portfolio company assets, etc.

At the crux of it, an office manager should not have the same access to information as the Chief Financial Officer, and user provisioning and management practices should reflect that.

PRO TIP

Some firms opt to leverage self-service user provisioning systems, which allows users to administer their own access to certain applications, data, etc. as a means to reduce the burden on the IT team. This strategy can be exective for certain low-risk applications with minimal access to sensitive information but should not be employed broadly across firm systems.

10. Incident Response Planning/Procedures

Cyber incidents today come in many forms, but whether it be a system compromise at the hands of an attacker or an access control breach resulting from a phishing scam, firms must have documented incident response policies in place to handle the aftermath – and yet, many firms do not.

It's inevitable that your firm will face a security incident, and thus documenting the process for business impact and resolution will enable your firm to react swiftly and (hopefully) with little to no impact to operations.

As we highlighted in our first point on risk management and governance, the firm's security program should be enforced from the top down. The CISO and CSIRT will determine when to activate the incident response procedures and drive them forward across the organization. Depending on the severity of the situation, the team may opt to escalate the incident plan – particularly if they suspect an event has occurred as a result of sabotage or a targeted attack.

Ultimately, the goal of the incident response plan is to ensure the business is able to continue operating at full confidence and to minimize the risk and exposures of the firm externally – that includes on regulatory, financial, and reputational levels.

PRO TIP

Communication is critical during incident response, and we don't just mean to employees. There are a number of third parties who will also likely need to be notified and kept abreast of the firm's situation, depending on its severity and potential impact. Select at least one member of the CSIRT to handle communication on behalf of the firm – to notable and affected investors, third party service providers and regulators.

BluWave is an innovative B2B Intelligent Marketplace that uses technology, data, and human ingenuity to connect more than 500 leading private equity firms and thousands of proactive businesses with best-in-class, pre-vetted, third parties for critical due diligence, value creation, and preparing for sale needs. BluWave's invitation-only Intelligent Marketplace includes private equity-grade service provider groups, independent consultants, and interim executives.

Visit **www.bluwave.net** or contact **info@bluwave.net** for more information.

(615) 588-4010