White Paper

Finance Industry

Financial Sector Threat Landscape 2020

Financial organisations are aware of cyber threats. But the majority are unaware of the gravity of an attack until it is too late. Learn what to look for to stop an attack in its tracks.

→ securityhq.com

SecurityHQ

Table of Content

Executive Summary

Why the Financial Sector?

Within the global sector of cyber security, the two major areas that are constantly under attack are financial and governmental. Financial organisations that hold consumer data, in particular those that provide financial services to retail and commercial customers, including banks, investment companies, real estate firms, retail banking and insurance, are an obvious target for the simple fact that this is where the money is.

'Attacks in this sector are perpetrated by external actors who are financially motivated to get easily monetized data (63%), internal financially motivated actors (18%) and internal actors committing errors (9%).' - Verizon, 2020 Date Breach Investigations Report (DBIR).

The 2020 Verizon report further highlights that the reasons behind an attack can be broken down further, with financial gain being the reason behind 91% of attacks against the financial sector, espionage being the cause behind 3% of attacks, a grudge or revenge attack being the reason behind a further 3% of attacks and the remaining 3% being influenced by other causes.

Unless an attack is of a personal nature, in which the reputation of an individual or business is targeted, monetary assets are usually the endgame. And if there is a vulnerability in either processes, technology or team, it will be targeted.

> **'Cyber threats will continue to grow into 2021. That much is clear. Financial organisations have either already tackled a cyber-attack. Will tackle one in the very near future. Or may be a target of one currently but are simply unaware of the fact.'**
>
> Feras Tappuni, CEO, SecurityHQ

Security measures within banking have evolved dramatically, with regards to combining elements such as key codes, two factor authentication, voice ID, behavioural analysis, one-time passcodes, protective messaging, digital fingerprinting, and so on. But with more security measures in place, there are arguably more elements to infiltrate. In response, banks and financial institutions require tailored and sophisticated security to support their systems and people, and to defend against an onslaught of complex and aggressive cyber-attacks. Not only must security compliance within the financial sector be tenfold, but it is essential that security precautions evolve, to mirror the growing threat landscape.

But with threats growing in both size and sophistication, it is hard to know what to prioritise. Which is why this paper aims to provide some real-world context by, first, exploring a recent real-life attack on one of our larger financial clients, 'Bypassing Security Controls. Real-Life Example Explored.' Followed by an analysis of the five top threats to financial organisations presently. These being Internal Threats,Ransomware, App Developments, COVID-19 and Third-Party Risks.

> **'As they move forward, financial institutions will need to explore and implement a new blueprint,**
> **one that propels operations, customer relationships, security and compliance toward the**
> **different normal.'**
>
> IBM. *Banking and Financial Markets (2020)*

Bypassing Security Controls Real-Life Example Explored

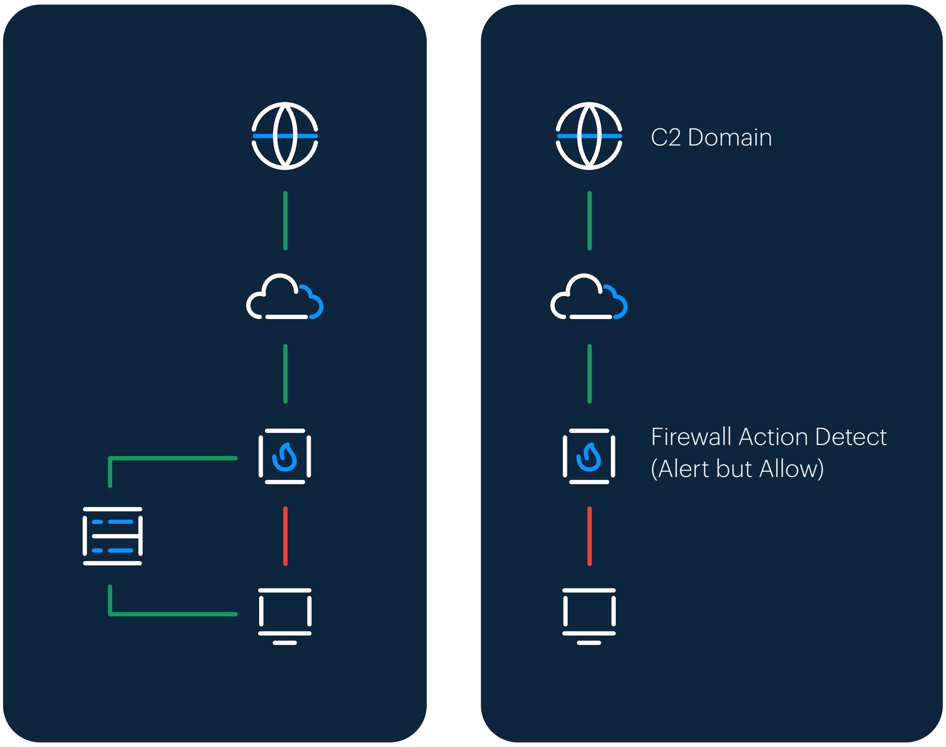
Incident Classification	Malware. C2
Actor	External
Action	MaliciousCode.Backdoors
Asset	Endpoint

Companies may have security controls in place. But if regular reviews are not conducted to ensure that security operations cannot be bypassed, then things can and do go wrong. More often than not, security controls and measures can be bypassed when simple procedures are not in place or forgotten. Which was just the case for one of our large financial clients, who was recently compromised by an old infection known by the name of 'Andromeda' or 'Gamarue'.

Andromeda was a trojan botnet malware that became apparent in 2011, for infecting approximately a million new machines a month. This specific malware was known for targeting Windows platforms, particularly in the communication, finance, insurance and manufacturing industries. A successful attack led to the theft of personal information, whilst also downloading additional malicious executables in the process. The key issue with this malware, however, is in the fact that Andromeda uses RC4 keys to encrypt data. Naturally, this makes it very diicult for security systems to detect the issue in the first place. And while this specific malware is no longer an active threat and was eradicated by the FBI and Europol's European Cybercrime centre (EC3) in 2017, what we often find is that many systems are still infected, especially on original scripted C2 servers.

This was just the case with regards to one of our clients in the financial sector, in which command and control tunnelling methodologies, particularly DNS tunnelling, was exposed.

When analysing security procedures, what became apparent was that the client had the DNS security architecture in place but had simply forgotten to plug in a firewall rule to control any bypass. This meant that the endpoint systems were able to directly talk out to the internet over port 443, and that provided a path to bypass the DNS security architecture.



In an ideal world, what we want to see here is the green line only. We want to see a workstation server endpoint talking out to the DNS forwarder, which in many cases is often the active directory, pushed out through the firewall, with explicit policy to a configured DNS service. That is an ideal scenario. But here, we are seeing a bypass of those complete controls where firewalls don't have an explicit policy for DNS traffic. This meant that, along with the C2 traffic, the firewalls were allowing any traffic through.

How to detect abnormal tunnelling DNS C2 activity, and data exfiltration over those types of channels?

It comes back to catching the C2 behaviour. It's all scripted, so you need to check on the different paths, and look for any encoded URL's which do not mirror typical user behaviour. Also check by accessing any URLs which are not actually domain friendly names, but rather IP addresses. And type different ports other than 80/443.

Detect Abnormal Network Connections – C2 Activity

- Detecting base 64 encoded URL communication - "Vm0wd"
- Excessive URL access with IP addresses, typically on different ports than 80/443
- Excessive and repetitive URL Blocks – Excluding noisy CDN/Advertising categories
- Excessive traffic on "Uncategorized" web categories
- Repetitive connections to known malware/C2 sites
- Attempts to bypass the proxy – Excessive port 80/443 denies
- Attempts to bypass DNS forwarders – Excessive port 53 denies
- Beaconing- Excessive and repetitive URL access within a short time frame

In this case, what made this threat apparent was the repetitive connections to known malware/C2 sites. Identification of this can be hard. When malware and the C2 website is so old, it is not always easy to spot repetition feeds.

If we look into the timeline of this case, the firewall effectively had a policy feature that provided a list of bad domains and IP addresses, and could detect them. But what is also noteworthy, is that the actual name provided was instantly suspicious. No human would willingly decide to call a URL 'server2.39slxu3bw[.]ru'. So, had the firewall not triggered the activity in the first place, there are red flags to indicate a compromise.

29 Apr 2020 09:59

Connection attempts to domain "differentia[.]ru" and "disorderstatus[.]ru" "server2.39slxu3bw[.]ru" is seen at regular intervals.

29 Apr 2020 18:58

Connections Repetitive.
Started Seeing Action Detect for some of the traffic.

6 July 2020 09:37

DNS Architecture amended.
Firewall Signature Tuning Pending.

Initially, the bad domain names were being called out, and the UTM box prevented communication. But the important take away here is that this communication was all based on the reputation feed. And, after some time, we could establish that some of the connections were allowed and permitted on the firewall, simply because the firewall did not know what to do with that particular traffic. As a result, it just alerted and sent through that traffic. So, again, here is a case of where we could have hardened the firewall for specific signatures.

Another take away is that although this was a very old and known factor, still there were IP addresses that were allowed on the firewall. Which indicates that a repetition feed does not always highlight the issue.

In response, we blocked the malicious sites “differentia.ru” “differentia[.]ru” and “server2.39slxu3bw[.]ru” from Infoblox DNS. We then ensured endpoint security and ran a full vulnerability scan and latest patching.

Not a Quick Fix

To remediate such a problem requires architectural changes to the way an entire banking DNS service was configured. That's not a flip of the switch. To do this you need to identify the problem, demonstrate it with a security incident, or some compliance violations, and convince the customer that they need to change. That's not always an easy thing to do.

In this case, it took two months until we got our client to re-architect their entire DNS infrastructure. Which is good going for a bank. Allot of organisations aren't able to do that so quickly.

Take Away

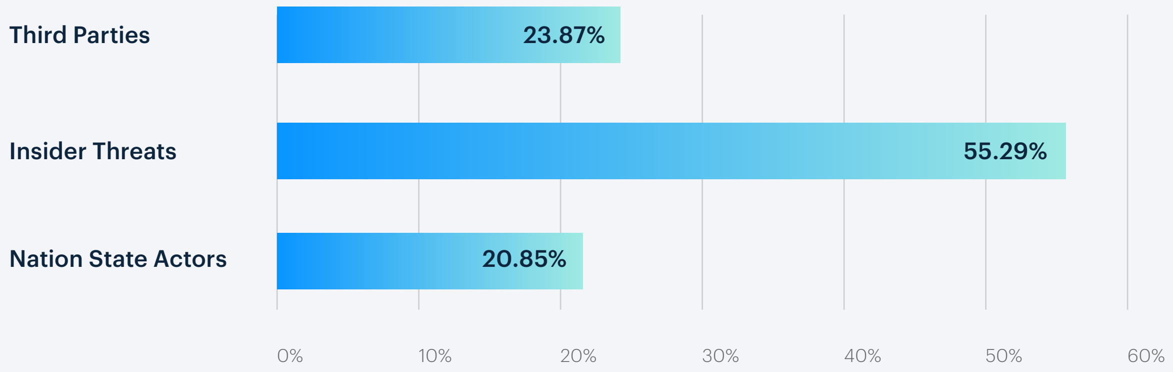
Incidents need to have lessons learnt, and lessons learnt need to be followed up in order to close them up quickly and efficiently. And we would not close an incident until we saw that the root cause of the problem was fixed.

While an organisation may have security controls in place, few organisations have the confidence in their security controls to work effectively when attacked. Therefore, conducting regular reviews and tests to ensure that security operations cannot be bypassed is crucial. And in this case, and despite the issues caused by the incident, everyone involved gained confidence in their security. First, by making the vulnerability and threat visible and, second, by knowing that the changes made to systems will continue to work for them.

Insider Threats

SecurityHQ recently released a poll, posing the question 'What Keeps You Awake at Night? Third Parties, Insider Threats or Nation State Actors?', to over 70,604 cyber security professionals. Over 55.29% of those who took part in the poll answered with Insider Threats. Followed by Third Party Risks, at 23.87%, and Nation State Actors at 20.85%.

What keeps you awake at night?



What Keeps You Awake at Night?
Third Parties, Insider Threats, or Nation State Actors? Survey Results Explored. SecurityHQ, (2020).

With '66% of organizations considering malicious insider attacks or accidental breaches more likely than external attacks.' (TechJury, *Insider Threat Statistics to Look Out For in 2020),* both malicious and accidental internal security breaches are a regular occurrence.

It can be argued that one reason why many cyber criminals know so much about the inner workings of financial organisations is because, at one point or another, they may have worked legitimately within the industry. But while some attacks are vindictive, the issue that we are regularly seeing within Finance, is that many employees/insiders are completely unaware that they are a threat in the first place.

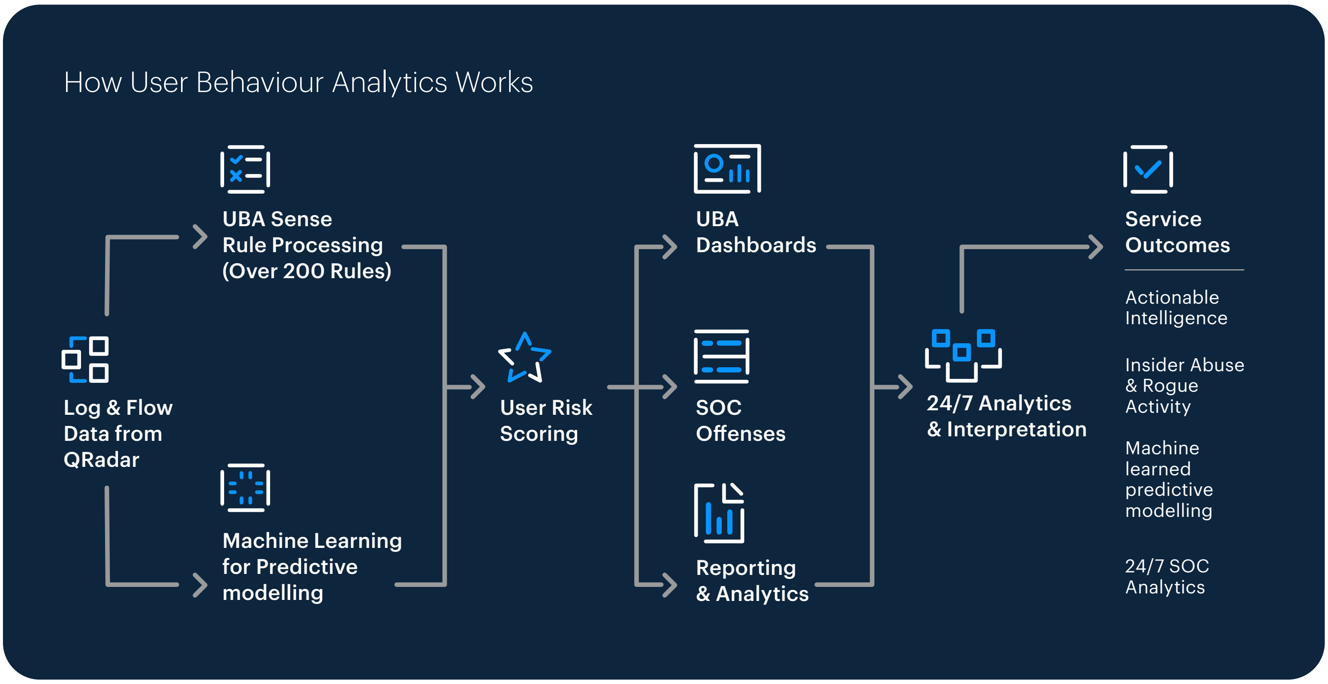
Take, for instance, an employee working remotely. This employee may be working with a company device. If this device was unknowingly hacked while using a different Wi-Fi, the user may be completely unaware that they are spreading malicious malware via their device throughout the company. And, due to current COVID-19 conditions, with over '30% of people now working remotely full-time, and an additional 18% working remotely one to three times per week.' (OwlLabs, *The State of Remote Work Report.* 2020), the more probable it is that a connection to an unsecure network will be made.

According to the Verizon, *2020 Data Breach Investigations Report (DBIR)* 'employees' mistakes account for roughly the same number of breaches as external parties who are actively attacking' the organisation. In fact, misdelivery within the company, by which information has inadvertently been sent to the wrong person, appears to be the most common issue within insider threats. Misdelivery can occur via emails forwarded or sent to the wrong person/recipient, or by incorporating the wrong mailing list, or via the wrong address on a paper document. Misdelivery is, more often than not, accidental and non-malicious, but the results can be devastating. Especially if sensitive data is inadvertently shared to the wrong recipient.

How to Reduce Insider Threats

First, security training is essential. Employees must be aware of the company's security protocols and measures, both in and outside of the office.

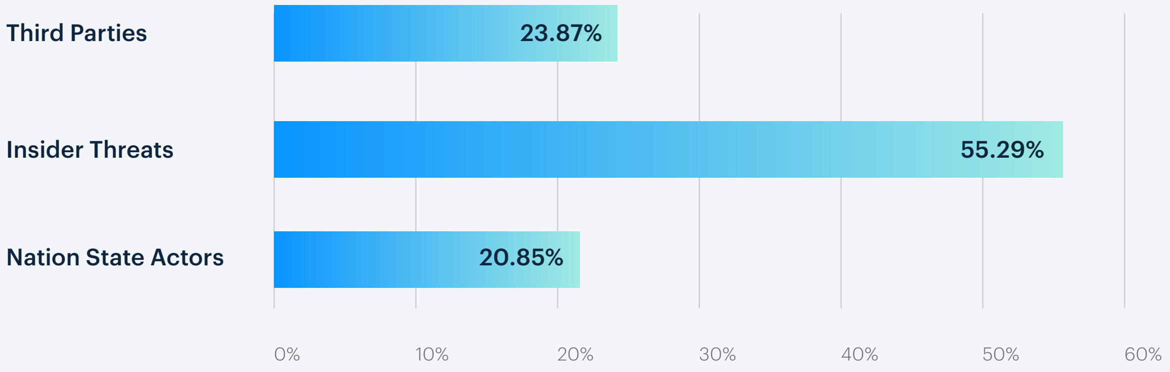
Second, User Behaviour Analytics (UBA) is essential to understand actions, and to highlight and stop unusual activity before the damage is done. By using ML algorithms, expert analysts are able to categorise patterns of user behaviour, to understand what constitutes normal behaviour, and to detect abnormal activity. If an unusual action is made on a device on a given network, such as an employee login late at night, inconsistent remote access, or an unusually high number of downloads, the action and user is given a risk score based on their activity, patterns and time.


How User Behaviour Analytics Works
Log & Flow Data from QRadar
UBA Sense Rule Processing (Over 200 Rules)
Machine Learning for Predictive modelling
User Risk Scoring
UBA Dashboards
SOC Offenses
Reporting & Analytics
24/7 Analytics & Interpretation
Service Outcomes
Actionable Intelligence
Insider Abuse & Rogue Activity
Machine learned predictive modelling
24/7 SOC Analytics

Third-Party Risk

Following the results of the poll, in response to the question ‘What Keeps You Awake at Night?’, 23.87% of the cyber security professionals asked, responded with Third-Party Risk.

What keeps you awake at night?



What Keeps You Awake at Night?
Third Parties, Insider Threats, or Nation State Actors? Survey Results Explored. SecurityHQ, (2020).

These days, few organisations work on their own. The majority use third parties, including vendors, partners, e-mail providers, service providers, web hosting, law firms, data management companies, subcontractors and so on. With regards to many of these, from IT systems to sensitive information shared with legal teams, these third parties could easily be a backdoor into your financial systems for attackers to infiltrate.

According to the Ponemon Institute Report, '53% of organisations have experienced one or more data breaches caused by a third party, costing an average of $7.5 million to remediate.' For a large organisation, this can be crippling. And can wipe out a small organisation in a matter of minutes.

To manage third parties, financial organisations must have the ability to detect threats, and the capability to respond to them. Which requires the right combination of people, processes, and technologies.

But half the battle is locating vulnerabilities in the first place. Which is why cyber resiliency needs to be sharp, and why investing in the best managed security services is essential. From Firewall Management, to Decoy Deception and Honeypots, it is important to know what services will support an organisation best. This will depend on factors including location, company size, current security measures and more.

COVID-19

A key element to take into consideration over recent months is, of course, COVID-19.

Cyber criminals are continuing to target the financial sector amidst the pandemic. As a result, we have seen a spike in attacks on banks, financial organisations and the third parties connected to them. Before COVID-19, if an attacker wanted to sabotage a company or steal data, they would target the business itself. The website, the social accounts, the logins and all their vulnerabilities. In response, organisations had parameters set up for this. But now, you just need to target a single remote worker.

Plans have not been put in place for such events in any large scale, and the IT teams that companies rely upon, are now left to fend for themselves. Using, perhaps, not always the best methods. Because of this, aspects regarding remote working and disaster recovery plans have been rushed. And this is what criminals are exploiting.

VPN Attack

For the majority, VPN's are being used by remote workers across most organisations. These are crucial to form a level of protection for remote worker devices. However, the major issue here, is that most organisations were in such a rush putting plans in place for their teams to work remotely, that these VPN's did not/still have not passed the normal quality checks that you would expect. Some of these VPN connections were only initially meant for staff to dial into and were not intended for mass users. Now that everybody is using them, systems are under extreme pressure.

What Happens When a VPN is Attacked?

Say your company mail was to go down for a few days, due to the influx in traffic as the whole world works from home. This would be significantly inconvenient for the whole organisation. But can be worked around. But say a financial organisation of 20,000 employees is using a single VPN gateway. And let's now say that somebody does a denial of service, using a VPN remote gateway. Because processes were rushed, this system now crashes under the significant capacity, and goes down for 2 to 3 days. The amount this will cost an organisation is substantial.

What Does This Mean for the Future of Work?

It is reasonable, following the latest trends, to predict that such DNS disruptions and direct attacks of VPN gateways will increase. It is equally plausible to surmise that these attacks will be followed by extortion emails and campaigns. Including large scale phishing attacks.

How Should Organisations Reduce Threats?

Organisations need to ensure that they treat their VPN and remote workers properly. Often, for threats to get their foot in the door to lead to a VPN attack, they will start with dictionary attacks, attacks on cloud-based solutions, or phishing campaigns.

Our Initial tips:

- Implement a Remote worker policy and remember amendments, awareness.
- Do NOT leave you endpoint connected to the corporate network.
- If BYOD, ask to be responsible with corporate data, by:
    - Restricting corporate data to a single BYOD device.
    - Ensure regular patching
    - Only use BYOD with Endpoint protection AV/FW
- Be Vigilant
    - Think twice before going to a website (especially from mail). And do not click on anything you are unsure of.
    - Only get COVID, Corona information from trusted sources. Not via email or social media accounts.
- Understand the changes to the threat model. No remote access = Zero productivity.
    - Evaluate Fallback/Contingency
    - Test DOS protection / Capacity
    - Identify Threats/Vulnerabilities ... E.g. DOS against DNS

- Patch your perimeter!
  - Enforce/Implement MFA – Does NOT give significant service disruption.
  - Disable Interactive logon on ALL default user/service names.
  - Disable all accounts that have not been used for a significant period.
  - Maintain and implement a top 20 country blocklist (SecurityHQ maintains a top-20 based on risk models)
  - Implement audit related security controls and monitoring. Analyse these for threats.
  - Monitor remote worker behaviours: such as duration and access denied.
  - Attempt to implement more granular access control on critical data/systems.
- NO SHORTCUTS
  - No Backdoor for IT (like RDP, RAT tools)
  - No remote logins using privileged accounts
  - Implement / enforce Jump host for IT operations

App Developments

Apps surrounding investment and finance have grown substantially in 2020. This, in part, is a good thing, as the ability to invest online is quick and easy, and accessible to all. But due to the demand, many of these apps were developed quickly and are underprepared for cyber-attacks.

For instance, many do not provide two-factor authentication, are not supported by the appropriate regulations, are not patched or maintained properly, and do not have contingency plans in place to mitigate the effects of a cyber-attack. As a result, personal information of app users is relatively easy to steal and sell. This can be done by creating duplicate fraudulent apps to trick the user. On these duplicate apps, the imagery and language of the genuine app is mirrored. And, once the personal information is supplied, both real and virtual money is then accessible. Thus, the circle of ransomware ensues.

Mobile Banking

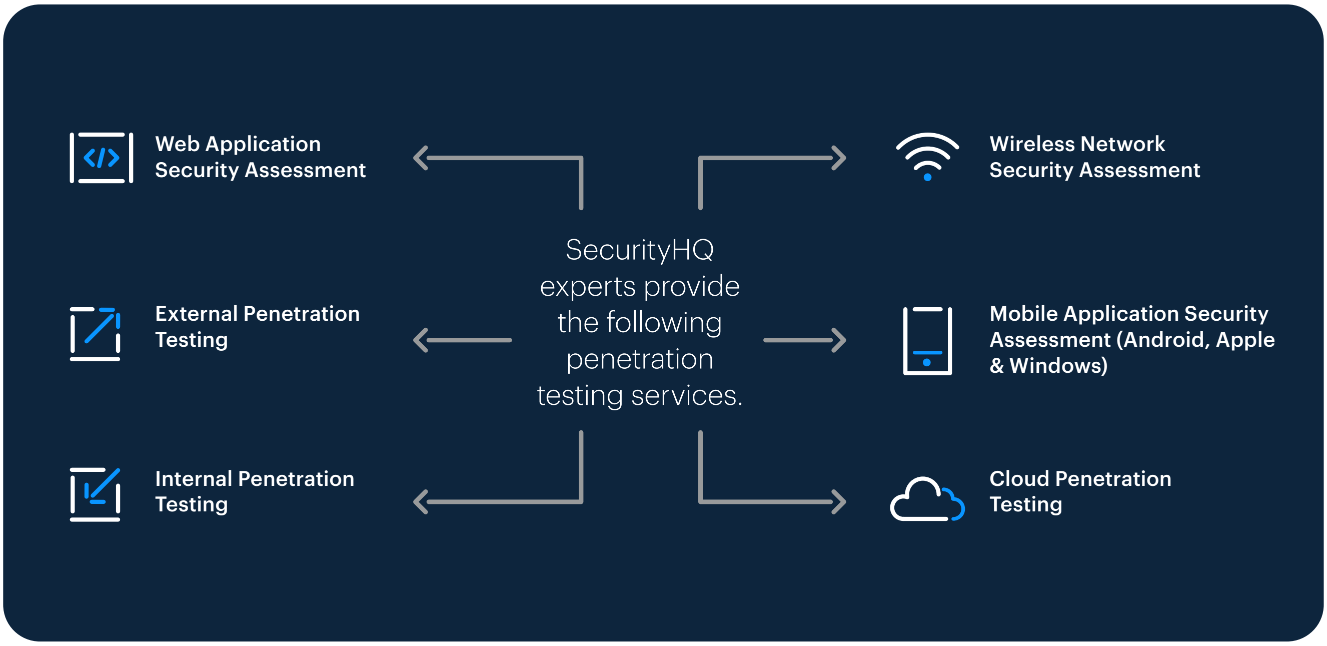
While traditional banking has security guards, bulletproof exteriors, cameras and more, online banking not only risks the user's money but personal details as well. Which is why elements including biometric authentication, two factor authentication and data encryption is used. While these elements may support the overall security, other components must be considered from the user's point of view.

Updates

Unlike a physical bank, the security of an app does not solely rely on the security of the organisation involved, but the user of the app as well. Users must maintain password security, and regularly update their apps to the newest version. The issue here is that there are only so many reminders an app can send to a user, and it is the responsibility of the user to make these updates. If they do not, accounts are vulnerable.

The Answer? Penetration Testing

Penetration Testing is used to hunt for, and highlight, vulnerabilities in networks by emulating real-life external and internal attacks. This way testing is conducted in a controlled environment, without compromising routine business activities. And issues, including identifying existing and potential vulnerabilities, are addressed.



SecurityHQ experts provide the following penetration testing services.

- Web Application Security Assessment
- External Penetration Testing
- Internal Penetration Testing
- Wireless Network Security Assessment
- Mobile Application Security Assessment (Android, Apple & Windows)
- Cloud Penetration Testing

Ransomware

> **‘90% of all financial institutions have experienced ransomware in the past year’**
>
> betanews.com

The term Ransomware is relatively new. Added to the Oxford English Dictionary only three years ago, it signifies the branch of malware that demands payment after infecting a computer. But, in the three years since being added to the dictionary, ransomware has increased dramatically both in terms of the number of attacks, but also in terms of the range of methods used to conduct said attacks. And because there are now many varying methods of incidents, we know, and can guarantee that it is not just large organisations that are being targeted.

> **‘Ransomware maintains its reign as the most widespread and financially damaging form of cyber-attack.‘**
>
> Europol Director, Catherine De Bolle.

Say a crime group has gained access to personal accounts. The next logical step is to blackmail the organisation via ransomware. Unfortunately, as a public security breach would cause mass panic and potential lawsuits, banks will often pay off cyber criminals into an anonymous cryptocurrency account, rather than lose client data. Crime groups know this.

The issue is that many organisations who pay criminals, in the hope of getting their data back, just make themselves more vulnerable in the process. Once money is paid, bad actors know that the organisation can be forced into a position to pay again. There is also no guarantee that data will be returned after payment, which means that the risk of both data loss and substantial monetary loss is probable. What’s more, systems will still be infected with malware following a payment.

Sometimes victims speak out, but this does not always end well. Take Travelex, the currency exchange company, for instance. Following an attack by a Sodinokibi ransomware in January, $6 million was demanded in exchanged for 5GB of personal data. Since the attack, Travelex has fallen into administration, with PwC saying that the ‘foreign exchange firm was acutely impacted by COVID and the recent cyber-attack.’

For financial organisations, ransomware can and will destroy a whole business.

> **“The threat vector of ransomware is definitely concerning for the industry, not only for us as a bank but for the industry and not only for the industry but also for the regulators.”**
>
> Saul Van Beurden, Head of Technology at Wells Fargo

To Pay or Not to Pay?

This is purely a business decision. But it is crucial to remember, whatever the business decision is, that there is no honour amongst thieves. Attackers are extremely sophisticated. Once they have your data, there is no guarantee that if you pay them off, that your data will be given back or decrypted. There is also no guarantee that you will not be a target a second time around. Often, once an attack is made, the bad actor will sell the details on to their associates to come after the victim again after deployment, because the payload can still be there, activated and deactivated.

What to do?

In the end, the best way to respond to a ransomware attack is to avoid having one in the first place. Backup data regularly. Scan the network infrastructure for vulnerabilities and patch the latest security updates to avoid ransomware infection. That way, if attacked, you can ensure that your downtime and data loss will be minimal.

> **‘Taking proactive measures early on can help organizations avoid the costs that come with a cybersecurity breach.’**
>
> IBM, *Assessing Cyber Risk in M&A*. (2020)

View and act on all vulnerabilities across all your digital platforms, including internet, applications, systems, cloud and hardware. Identify your weak points, monitor your online identity, verify issues, and remediate in rapid time with vulnerability management.

- ✓ Make Risks Visible and Avoid Costly Data Breaches
- ✓ Monitor Industry Specific Threats
- ✓ Measure & Track Your Digital Footprint

Considerations

Cyber threats within the financial industry will continue to grow into 2021. That much is clear.

Financial organisations have either already tackled a cyber-attack. Will tackle one in the very near future. Or may be a target of one currently but are simply unaware of the fact.

The financial sector has a lot to defend against. Everything from miscellaneous errors, privilege misuse, crimeware, web application attacks, denial of service attacks, cyber espionage, lost and stolen assets, payment card scammers, the list is endless. From external threats, internal threats, partner threats, and multiple threats each with motives covering everything from financial gain, espionage, and grudges, and with each attack risking personal data, credentials, banking infrastructure and more, the financial sector has a lot to protect and even more to lose.

> **“In the finance sector, you need to be on the front foot with regards to being agile enough to respond to the changing threat landscape. You need to have the tools and the people in place to protect you. Successful security is not about being lucky, successful security is about being ready, and being brave enough to make the changes that are required.”**
>
> Feras Tappuni, CEO, SecurityHQ.

In the end, effective security comes down to three key elements. Processes, people and technology. Processes must run seamlessly alongside the organisation. Security experts must have the capability to detect, react and understand the context of a risk. And the technology must be superior, to keep up with cyber threats. All elements are equally as important, and you must have all three to ensure security.

Best Practices to Avoid Being a Target

- Back up your computers and servers regularly.
- Secure mapped network drives with a password and access control restrictions.
- Educate employees on the latest email phishing scams and social engineering.
- Avoid handling files or URL links in emails, chats, or shared folders from untrusted sources.
- Update your anti-virus solutions with the latest virus definitions.
- Keep your operating system, network, and security devices at the current release patch update.
- Run software with the least privileges.
- Monitor your endpoints 24×7 by deploying EDR technology to detect advanced cyber-attacks.
- Have business continuity plan in place to endure user downtime.
- Align with better IT security practices and tools.
- Associate insurance policies that cover cost in case of an attack.

In times like these security measures are more crucial than ever. Especially for those within finance. So that our life savings are secure, the security of our loved ones is maintained, and the livelihoods of those employed within the financial world continues.

Contact SecurityHQ for a free assessment and consultation regarding your security risks and threats.

How Does SecurityHQ Differ?

Founded over 15 years ago, SecurityHQ is a Global MSSP that monitors networks 24/7, to ensure complete visibility and protection against your cyber threats. Threats can be both external and internal. Which means that the right combination of tools, skills, people, and processes are essential to manage, detect and defend your environment from all malicious activity proactively and effectively.

Our mission is to provide world-class security operations to our clients and partners, to integrate processes seamlessly, and act as an extension of our user's own teams. The result is a bespoke service that seeks to address the user's specific risks and challenges that empowers their cyber safety.

Bespoke

Every customer is different. Your risks, industries, geolocations, regulatory requirements and processes demand a bespoke response. SecurityHQ customises your services, based on your requirements.

Business Intelligence

SecurityHQ relates all incidents to CIA impact against your systems, data and users.

Integrity & Transparency

SecurityHQ build relationships on trust, built on a foundation of complete transparency in our operational delivery.

Incredible People

Our analysts are some of the most experienced and qualified in the industry.

Incident Management Platform

Collaboration is critical for effective security operations. SecurityHQ's Incident Management Platform is an arena for incident workflows, SLA management, data visualisation and documentary repository.

World's Best Technology

We only use Gartner Magic Quadrant technology, such as IBM QRadar, Resilient, X-Force.

Global Reach

SecurityHQ operates 6 Security Operation Centres globally and has unrivalled regional expertise with international oversight.

Personalised Service

Clients receive dedicated Service Managers and Senior Analysts who are available 24/7, every day of the year.

Have a question? We would love to hear from you.

Safeguard your business, people and processes with SecurityHQ.

Reach us sales@securityhq.com

Europe	7 Greenwich View Pl, Canary Wharf, London E14 9NN, UK
APAC	Supreme Headquarters, 807-810, Baner, Pune 411045, India
Middle East	Al Barsha Business Point,501, Al Barsha One, P.O. Box 283996, Dubai, UAE

Follow us f in 🐦

About the Author

Eleanor Barlow,
BA (Hons), MA.

Content Manager

As an experienced named author and ghost writer, Eleanor specialises in researching and reporting on the latest in cyber security intelligence, developing trends and security insights.

✉ Eleanor@securityhq.com

Appendix

- Barlow, Eleanor. *The Financial Industry Needs to Get Real About Security. SecurityHQ, (2020).* [https://www.securityhq.com/blog/the-financial-industry-needs-to-get-real-about-security/].
- Barlow, Eleanor. *What Keeps You Awake at Night? Third Parties, Insider Threats, or Nation State Actors? Survey Results Explored.* SecurityHQ, (2020). [https://www.securityhq.com/blog/what-keeps-you-awake-at-night-third-parties-insider-threats-or-nation-state-actors-survey-results-explored/].
- De Bolle, Catherine. *Internet Organised Crime Threat Assessment (IOCTA) 2019.* Europol, (2019). [https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019].
- Deyun, G. 20. *Insider Threat Statistics to Look Out For in 2020.* TechJury, (2020). [https://techjury.net/blog/insider-threat-statistics/#gref].
- Europol. ANDROMEDA BOTNET DISMANTLED IN INTERNATIONAL CYBER OPERATION (2017). [https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation].
- Hambleton, Aaron. *Notes from the Field. Don't Default on Password Security.* SecurityHQ, (2020). [https://www.securityhq.com/blog/notes-from-the-field-dont-default-on-password-security/].
- OwlLabs, *The State of Remote Work Report.* (2020), [https://www.owllabs.com/state-of-remote-work].

  Ponemon Institute Report (January 2020), [https://www.ponemon.org/].
- Van Beurden, Saul. *Timely Reminder About Who Bears Responsibility for Cloud Security,* AmericanBanker (2020), [https://www.americanbanker.com/news/timely-reminder-about-who-bears-responsibility-for-cloud-security].

- *Verizon, 2020 Data Breach Investigations Report* (DBIR) (2020).
- Ian Barker. *90 percent of financial institutions targeted by ransomware in the last year.* Betanews, (2018). [https://betanews.com/2018/05/22/financial-institutions-ransomware/].
- IBM. *Banking and Financial Markets* (2020). [https://www.ibm.com/thought-leadership/institute-business-value/industry/banking-and-financial-markets?lnk=hm].
- IBM, *Assessing cyber risk in M&A*. (2020). [https://www.ibm.com/thought-leadership/institute-business-value/report/cyber-risk-mergers-acquisitions?
- SecurityHQ, *Decoy & Deception Honeypots Service.* (2020), [https://www.securityhq.com/services/decoy-and-deception-honeypots-service/].
- SecurityHQ, *Managed Firewall.* (2020), [https://www.securityhq.com/services/managed-firewall/].
- SecurityHQ, *User Behaviour Analytics.* (2020), [https://www.securityhq.com/services/user-behavioural-analytics/].
- SecurityHQ (2020), [https://www.securityhq.com/].