AN INDUSTRY REPORT 2021

Achieving Cyber-Resilience in Financial Institutions

CEO • DIGITAL

DELL Technologies

vmware®

EXECUTIVE SUMMARY

Financial Services Industry (FSI) firms of all shapes and sizes are at greater risk of data breaches than ever before – even small FSI firms handle large quantities of sensitive data on a regular basis. The precarity of handling this data means that any amount of information leaked into the public sphere could potentially cost millions, if not billions, and the outcome would be extremely damaging.

A closer look is needed at how modernizing digital infrastructures can assist the shaping up of cyber resilience within financial industries for 2021 and beyond.

CEO.digital partnered with Dell Technologies and VMware to ask the C-Suite their thoughts on the state of IT within FSI to try and understand what the common goals and challenges are.

These are our findings.

INTRODUCTION

Last year, many businesses had no choice but to close offices and move to remote settings, causing a sudden, critical reappraisal of the modern workplace. How were companies going to share, collaborate, manage, or even just undertake simple communications and basic tasks by means of their newly distributed workforce?

The shift in market expectations caused by the pandemic has also made finance more of a target for hackers and fraudsters, with digital channels now being the primary mode of interaction between financial institutions and their customers. All this phenomenal, newfound interconnectivity has globalized the economy further and enabled financial services to stay standing, but it does have a flip side. It has created a black-hole of increased cyberthreat severity — with a greater online surface area, there is greater risk to organizational security.

It means that data protection is top of mind now. Ransomware attacks are being carried out, even Phishing scams have risen as people are spending more time at home and have upped their screen-time, all costing organizations millions of dollars in data loss as well as irrevocable down time and loss of revenue. In CEO.digital's recent analysis of the global EY CEO Imperative Study 2021, just over half (51%) of respondents were focused on digital transformation in the coming years, while two-thirds (67%) look to cybersecurity. So, in terms of ever-evolving digital transformation, FSI must become more vigilant than ever and stay on top of their infrastructures to combat increasing cyberattacks.

Organizational resilience should be top of the agenda for all FSI firms. This can be achieved through a technology strategy reshuffle and new cloud solutions that take the stress out of ensuring your company is cyber secure, not only to avoid customer data misconduct, but to stop economic downfall on a wider scale.

Our recent research and survey shone a light on the state of IT within the financial sector. The IT leaders who responded defined four key areas of focus for FSI firms looking to establish cyber resilience within their companies.

Want to find out more on Digital Transformation?

What can IT, Digital and Transformation leaders do to accelerate and optimise their digital strategies? Dell Technologies investigates in a new series of thought leadership and roundtable discussions.

Visit the innovator portal on CEO.digital to read industry reports, attend C-suite events and listen to podcasts on digital transformation, brought to you by thought-leaders Dell Technologies and VMware.

Visit The Portal →

CHAPTER 1

Security Culture: Providing a Masterclass in IT

One of the best ways to ensure your organization maintains a bulletproof cybersecurity strategy is through corporate culture. Leading organizations establish their cybersecurity resilience by reducing ambiguity and permeating a security mindset throughout the company. Without this cultural dynamic, businesses are likely to be more permeable to security threats.

Fortunately, new research states that finance and banking have the best security culture globally. The Financial Conduct Authority in the UK found that 90% of FSI firms have cyber awareness programs in operation. Whilst this statistic is reassuring, and likely reflected in the US and European markets, the FCA also expressed that due to security being one of the most fundamental elements in FSI, this number should most certainly be higher. Studies also show that despite finance taking the lead for their embedded security culture in comparison to other industries – in terms of having a 'good security culture' – finance has still not hit the mark.

FSI firms have pointed to another hurdle: the identifying and managing of 'high-risk staff'. Even where these high-risk roles have been identified, less than half of the IT leaders asked were confident they provide appropriate, additional cybersecurity training for these employees. In the CEO.digital survey with Dell Technologies and VMware, IT leaders from the finance sector were asked what they could do to further secure their business

> **"Even the best programs and technologies aren't enough if our employees don't play an active and informed role. That's why we're also committed to building our "human firewall" as a core component of our defense strategy."**
>
> **Mark L. Mullinix**
> Interim President and
> Chief Operating Officer,
> Federal Reserve Bank of Richmond

infrastructure. Around half stated they should offer more training to their employees.

Security principles must be embedded within organizations as not just an IT approach but a people's education. In the words of Mark L Mullinix, the Federal Interim President of The Federal Reserve 2017, "even the best programs and technologies aren't enough if our employees don't play an active and informed role. That's why we're also committed to building our "human firewall" as a core component of our defense strategy."

In realizing a positive security culture, finance leaders can build on brand value and customer trust, positively impacting overall business success. Unfortunately, what a security culture is hasn't been universally defined within FSI. Although 94% of leaders believe security culture is important, they have not agreed on what the term means and in a survey of 1,161 IT decision makers, 758 definitions were offered.

The CEO.digital, Dell Technologies and VMware survey did, however, show some common denominators in identifying what a security culture means.

But it's worth bearing in mind Security Awareness Advocate Javvad Malik's warning that "all of these dimensions are inextricably interlinked; should one falter so too would the others." With due care given to each aspect, FSI organizations look set to create a resilient security culture that stands the test of time.

- **ATTITUDE**
  Formed over time and through experiences, individuals must cultivate their own opinions reflecting the security protocols of the business
- **BEHAVIOUR**
  When the time comes, individuals make physical actions and decisions based on their learnings which impact the security of the business
- **COGNITION**
  Attitude and behavior are meaningless unless there is an understanding and knowledge of threats
- **COMMUNICATION**
  The channels and methods used to share security-related information in a timely manner that supports employees when needed
- **COMPLIANCE**
  Clearly vocalized and written security policies and the extent that employees adhere to these

CHAPTER 2

Why Good Corporate Governance is Key

Governance is another cybersecurity essential; the survey revealed that C-Suite leaders view it as one of their major concerns. More prominent was not the concern itself, but that of FSI firms being overconfident about their ability to meet governance expectations. Reports show that 20% of operational incidents were explicitly linked to weaknesses in change management, suggesting a telling disparity between expectations and reality during these shifts.

Setting up a Zero Trust model is in high demand amongst the savvy financial firms of today. This modern approach to cyber security stems from a 'trust no one' outlook both externally and internally. It means that all employees have the least amount of privilege necessary to carry out their work effectively and every person or device requires strict verification before granting access.

But most of the time, FSI cybersecurity governance plans consist of a logical, albeit outdated 'weakest link' strategy. This approach focuses on alleviating specific, individual risks and whilst it works, it just doesn't hit the mark in terms of how quickly these security threats evolve. That is where good governance comes into action. Having a cohesive and malleable approach that considers people, technology, process and compliance is a sure-fire way to stay protected.

So, aside from making sure the appropriate new technology is utilized, it isn't just large IT movements that lead to security

> **We are looking for firms to have good governance around cybersecurity in their firms – by this, I mean senior management engagement, responsibility – and effective challenge at the Board.**
>
> **Nausica Delfaas**
> Executive Director of International and Interim Chief Operating Officer, Financial Conduct Authority

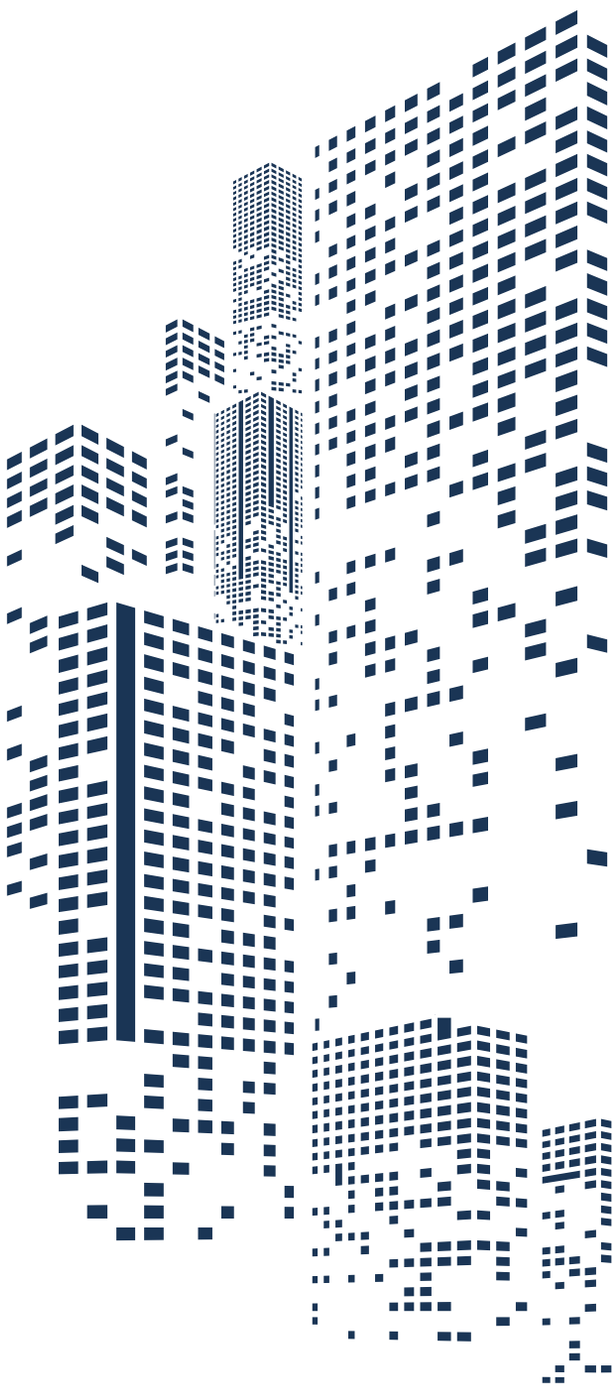
issues. Leaders also need the adequate knowledge and skills to implement, maintain and govern their systems and processes and these leaders fall under two strands:

- **Senior managers**
  The day-to-day, physical, action-oriented side
- **Board members**
  Not just the daily tasks, but a more due-diligence, strategic oversight

Research suggests that Senior Managers and Board members should look to these key markers for ideas on good governance:

- Establish the current state and assess where existing risks lie — this is especially important in finance where the evolving technology and data is causing more loopholes than ever
- Review, update and create all cybersecurity policies
- Approach cybersecurity from a business angle, understanding what data needs protecting within the context of the business
- Increase awareness and training for all employees across the board
- Analyze your cyber risks by constantly monitoring, measuring and improving

Once the C-suite begin to understand cybersecurity as a management initiative, they'll establish a better cybersecurity approach for the entire business.



CHAPTER 3

Data Explosion Linked to Cyberattacks

Big data is the primary enabler of digital innovation in the financial services sector today. But one of the challenges posed by it is the fact that data itself begets more data. Some estimates suggest the world creates roughly 2.5 quintillion bytes of data every day. With so much to manage, it's only a matter of time until a major security breach occurs.

Our survey respondents agreed. Financial leaders feel that the exponential growth in data poses a security risk in the future. The sharp rise in popularity of digital channels will certainly increase the amount of data users produce – and FSI firms benefit from. For instance, in 2020, the European Commission noted that just after the Covid-19 pandemic started, the use of finance mobile apps in Europe increased by 72% in just one week. At the same time, cyber-attacks on firms rose by a startling 38%. This explosion of sensitive data in the cloud, mobile and other environments is seeing rising cases of hackers and fraudsters trying to exploit it, which is why cyber security has become a top priority for financial service leaders worldwide.

On a side note, it's worth mentioning here that whilst this data growth does possess increased risk overall, it's not just business data that's risen – there's also been abundant growth in behavioral data. This allows systems to distinguish anomalies or review access policies, aiding cyber security for organizations.

With A Greater User Base comes Greater Risk

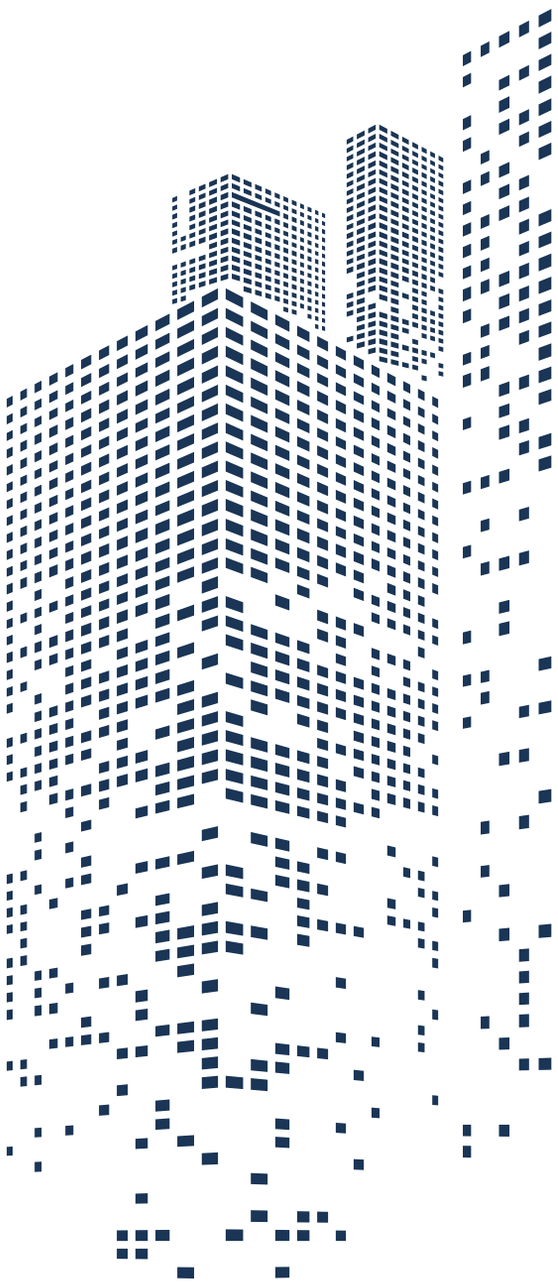
Increase in the use of finance mobile apps

Number of cyber-attacks on firms

This might be something to look at alongside implementing Big Data management tools such as these as a part of cyber-resilience strategies.

- Properly discarding of old assets as they bring in new technology. Many of these assets will contain exploitative data. So, it is critical that FSI firms dispose of these carefully when doing so.
- Encryption and virtual private networks involving securely encrypted cloud-based services for all internal operations – storing everything together can make things more manageable.
- Better staff training of clearer cybersecurity policies that state what information is confidential versus what can be shared as well as, from a technological perspective, what devices can be used at work, what can be taken home and what appropriate usage of the device looks like.
- Both built-in security and integrated data protection to ensure that data is secure when at rest, or in use or when shared across devices, data centers and in the cloud, such as installing a firewall as a frontline defense mechanism (and making sure it's updated regularly).
- Use a multi-factor authentication as an extra security step on top of standard password – some FSI firms are using second passwords, fingerprints, facial recognition etc.

These steps should all be taken on board in order to mitigate risks and detect suspicious activities. In this way, FSI firms take one step closer to true cyber resilience.



CHAPTER 4

The Banking of the Future

The financial markets are ripe for innovation, but some organizations struggle to implement change correctly and leave themselves open to new risks.

On the one hand, this pace of innovation has been a good thing, bringing about a true revolution in the way the FSI sector works. Our survey revealed that almost all C-Suite leaders fully understand the need for innovation, and the idea of investing in new initiatives no longer comes up against the resistance it once faced. However, the survey also stated that half of these decision makers do not know what systems or applications to prioritize — a big challenge of 2021.

So, what are the core digital strategies that IT leaders should be prioritizing?

FSI has been massively reshaped by means of AI (Artificial Intelligence) and ML (Machine Learning) which are already causing waves in the industry. AI is improving FSI with smarter, faster decisioning processes. For example, developing solutions to assess the credit worthiness of borrowers, better risk management from AI algorithm predictions, and through use of a combination of cloud-based and on-premises AI, FSI firms will be able to focus on combating different risks like fraud and money laundering.

It will also have a large-scale impact in Trading for ranking stocks, generating forecasts, analyzing data and identifying patterns.

Technology partners come in many shapes and sizes, but there are two that should be considered a priority: service providers that make it their business to host, secure and manage analytics or cloud-based programs and development partners that are willing to work hand-in-hand with a bank to ensure maximum security across the business.

Falk Rieker
GVP, Global Head,
IBU Banking

Meanwhile, investments in conversational AI as virtual finance assistants in the personal banking space is only going to get more popular.

There has also been innovation in these spaces:

- Mobile banking usage has rocketed by a massive 200% since the start of the pandemic, as customers flocked to digital channels for all their everyday banking needs. Expect more investment in this space, which will require new infrastructure to support even greater functionality on-the-go.

Mobile banking usage increase since the start of the pandemic

- Customer Experience, underpinned by greater value extraction from vast data pools the sector has collected. Using big data, FSI firms will train ML algorithms to bring enhanced personalization to consumers, even automating many basic processes to further streamline the experiences.

- Embracing cloud computing as a route to outsource data storage and access advanced software, as well as helping innovate process and reduce costs on multiple levels – Cloud migration saves around 15% on all IT spending, with small to medium sized businesses saving up to 36%.

IT savings with cloud migration

- Robotic Process Automation (RPA) describes a virtual workforce that streamlines business processes by completing administrative duties usually carried out by employees – generating higher ROI and boosting productivity. It's said that 80% of FSI leaders have made plans to implement RPA in the near future.

of FI leaders plan to implement RPA

- What about the outpost of cloud extended to the edge? In a next wave of AI, Edge Computing is forecasted to reach 1.12 trillion by the year 2023. Drivers of this include privacy, as customers are becoming more aware of where their data is located, and better security through multiple layers of encryption. Most importantly, Edge Computing promises to reduce latency immensely as service distribution between network and devices is greater, not just mobiles and laptops, but IoT devices too.

Aside from these basic go-to's of new digital strategy, FSI firms should heavily consider their need to find the right technology partner for them. Now, more than ever, it's essential to trust your technology partner when it comes to protecting your company. According to Falk Rieker, a senior level financial services professional: "Technology partners come in many shapes and sizes, but there are two that should be considered a priority: service providers that make it their business to host, secure and manage analytics or cloud-based programs and development partners that are willing to work hand-in-hand with a bank to ensure maximum security across the business."

If IT managers step up their communication strategy and introduce all digital changes to all employees, then a seamless, low risk move into the future of banking will look likely.

LOOKING FORWARD

Financial Services firms are moving in the right direction around security breaches, but it's evident there is room for improvement because despite C-Suite leaders' awareness that technology modernization is the future of banking, they are not necessarily giving it their full attention.

For traditional banks and finance services to prosper, they need to be both taking specific steps towards building better cyber security in the face of distinct challenges. They must also make certain their facilities and customer experience match that of newer Fintech banks who are already providing this, without compromising on compliance. Failure to do so could see traditional enterprises head towards a huge loss - and it's the digital native challenger banks that will take over.

Top FSI firms are now those that are finding, preventing and solving breaches and are doing so through better training, bigger collaboration and correctly sourced technology investments such as end-to-end cloud solutions. Resilience is a business necessity in FSI that needs to be seen not just as an IT issue, but as a company-wide asset and business initiative. With the right processes and attitude, it can be achieved.

CEO
• DIGITAL

For more leading insights from around the world, join thousands of C-Suite leaders in benefiting from CEO.digital online and on social media now.

in partnership with

DELL Technologies vmware®