

Sponsored by



In Financial Services, IT Has Little Confidence in Users Keeping Customer Data Safe

It's time to recognize user needs and secure them

An overwhelming majority of IT professionals in the financial services industry are not confident that their employees, consultants, and partners are taking adequate measures to secure their customers' data, according to research commissioned by BlackBerry.

While security and compliance concerns around file sharing and mobility continue to cause headaches for IT organizations in financial services, the research also examines how the sector's plans around emerging technologies will introduce new areas of risk in the future.

All told, **94 percent of more than 500 financial services IT professionals surveyed from across six countries in North America and Europe say they are "not at all confident" or "somewhat unconfident" in the ability of their employees, consultants, and partners to adequately safeguard customer data.**

File sharing is a particularly vulnerable part of the security landscape in financial services, with three-quarters of respondents saying their organization experienced negative consequences as a direct result of insecure file-sharing practices (Figure 1). Lost productivity is the most cited consequence of improper file sharing, followed closely by compliance penalties.



The Most Secure Enterprise-Grade File Sync & Share

Provide employees with access to documents when and where they need them, and on any device, without fear of data leakage.

BlackBerry® Workspaces is the best choice for secure file sharing and file transfer.

- Control access to any file, even outside your firewall
- Enable collaboration from any device between internal and external contacts
- Revoke access to any file or by any user, even after the file has been downloaded

In this Paper

- File sharing is a particularly vulnerable part of the security landscape in financial services
- Many employees in this sector have to work around corporate IT policies to get their jobs done
- Secure, easy-to-use applications that support collaboration and connectivity will help address these risks

Has your firm experienced any of the following due to insecure file sharing practices?

Consequence	Percent of respondents
Lost productivity due to redundant efforts	74%
Penalties for compliance failure	70%
Exposing sensitive data to the competition	31%
Impact on the brand because of a data breach	22%
None of the above	25%

Figure 1

Despite the lack of confidence in employees to protect sensitive data, security and compliance are, unsurprisingly, top-of-mind issues for IT professionals in the heavily regulated financial services sector. The survey found that **64 percent of respondents cite compliance as one of their organization's top three emerging challenges** (Figure 2).

What do you see as your organization's biggest emerging challenges? Choose your top three challenges.

Challenge	Percent including in Top Three Challenges
Regulatory compliance	64%
Keeping up with cybersecurity threats	43%
Quantum computing - quantum safe cryptography	42%
Mobile threat detection	34%
Providing greater flexibility through business collaboration	32%
Protecting privacy and data security	27%
Tech nimbleness of disruptive competitors (entirely new technology-driven business models and rising client expectations)	24%
Leveraging technology to improve overall network performance	19%
Balancing productivity needs with security requirements	17%
Innovation with Machine Learning/Artificial Intelligence (AI)	16%
Need for consolidation - Enable productivity across teams, clients and partners & manage your organization's diverse set of endpoints and apps (from a single console)	16%
Use of third-party systems	16%
Other	9%

Figure 2

Is IT Providing the Tools Users Need?

Security concerns are having a real impact on how financial services organizations deploy applications. According to the

survey, **80 percent are limiting in some way the deployment of applications as a direct result of security.**

- 57 percent of respondents say their organization is holding back on the deployment of applications that use sensitive data.
- 23 percent say they are limiting deployments of some applications to business-critical or executive users



Protect Enterprise Data with Industry-Leading Containerization

With a growing number of employees using their own desktops, laptops and tablets, BYOD is gaining momentum beyond smartphones. BlackBerry® BYOD products offer flexible solutions for all your evolving device, app and content management needs that deliver maximized productivity, reduced costs and enjoy unparalleled security.

• Prevent data leakage

Keep corporate and personal data separate and block unauthorized devices from accessing your network with **BlackBerry® Dynamics**.



• Maintain user privacy and IT security

Enable access to corporate email, calendar and more, without sacrificing security with **BlackBerry® Work**.



• Secure Web Apps and Internet Access

Give your organization mobile access to your intranet and corporate network via a secure browser with **BlackBerry® Access**.



An important aspect of file sharing and collaboration is the ability of employees and partners to work securely using productivity applications sanctioned by the IT department. When such applications are not available, or are difficult to use within existing business processes and workflows, users will often look elsewhere for tools that help them get their work done. Whether file-sharing applications or other productivity tools that help employees and partners collaborate, these so-called "shadow IT" apps are often a concern to IT organizations that cannot control

access to information when users store it in consumer-grade, often cloud-based repositories and applications.

According to the financial services IT professionals in the survey, **59 percent feel their employees have to work around corporate IT policies to get their jobs done** on a monthly, weekly, or daily basis. Nearly 50 percent of respondents said such workarounds occurred at least once a month (Figure 3).

How often do you think company employees have to work around the company's IT policies to get their jobs done? For example, emailing a document to a personal account so they can work on it at home, or being forced to bypass a corporate VPN.

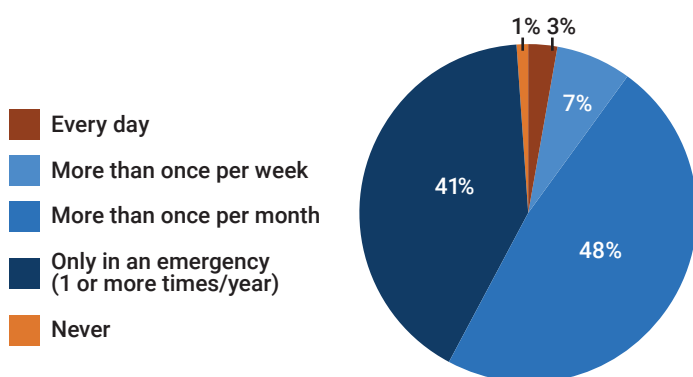


Figure 3

Circumventing IT policies has a strong correlation with IT professionals' confidence in users to protect sensitive data, the research found.

- Nearly two-thirds of the respondents who say they have "no confidence" in their users' ability to protect data also said their users had to work around IT policies on a daily basis.
- A similar percentage of respondents who were "very confident" in their users' handling of sensitive data said their users never had to work around existing IT policies.

Providing users with the applications they need increasingly includes providing mobile access to applications and data so that users can maintain productivity beyond the office. While 60 percent of the financial services IT professionals surveyed say their users have the applications they need to do their jobs and meet their business goals using mobile devices, the survey found strong evidence that mobility is a weak link in security strategies.

The signs are clear: mobility is an area where financial services IT department need to recognize the needs of users and address them with secure solutions. Among respondents who felt strongly that their users had access to the tools they need via mobile devices, only 6 percent also felt their users had to work around existing IT policies to get their jobs done more than once a week.



The Only Secure Option for Seamlessly Using Native Microsoft Apps

BlackBerry® Enterprise BRIDGE provides the only highly secure option for seamlessly using native Microsoft® mobile apps including Microsoft® PowerPoint®, Word and Excel® from BlackBerry® Dynamics apps such as BlackBerry® Work. Get the full native app experience and file fidelity desired by users on mobile devices with unparalleled security. This unique capability is available on both iOS and Android™.

Productivity vs. Security

Navigating the fine line between user productivity and security is a common challenge for IT organizations. For years, too many of the applications and other safeguards designed to help protect data and devices served as roadblocks to user productivity. This helped propel the adoption of shadow IT and thus decreased the level of security.

The survey data suggests the balance of productivity and security remains a challenge for IT organizations. While the financial services IT professionals in the survey identify security and

When considering the deployment of new industry apps and technologies, please rank the factors that impact your decision?

Factor	1: Most Impact	2	3	4	5: Least Impact
Does it make employees more productive?	71%	25%	1%	2%	2%
Is it easy for employees to use?	35%	14%	16%	19%	16%
Does it meet regulatory compliance?	21%	22%	15%	27%	15%
Is it secure?	14%	17%	34%	18%	17%
How much does it cost?	11%	31%	23%	21%	14%

Figure 4



Protect All Endpoints from a Single Console

Consolidate your endpoint management with trusted security across desktops, laptops, tablets, smartphones, wearables and IoT nodes with **BlackBerry® UEM**.

- Data protection at the device, app and content level
- Device, OS, app and user-based policies
- Unified, Multi-OS Endpoint Management with support for iOS, Android™, Samsung Knox™, Windows®, macOS, BlackBerry®, watchOS, and Android™ Wear

compliance among their top emerging challenges, productivity and ease of use rank higher than security, compliance, and even cost when it comes to factors that influence their decision to deploy new applications and technology (Figure 4).

IT professionals in the financial services sector also recognize the challenges of making applications accessible to users in the modern IT environment. More than three-quarters of the survey respondents strongly or somewhat agree that deployment effort across multiple devices and application management solutions is an important consideration when deciding which applications to deploy.

Why the discrepancy between security and compliance and the factors that influence the tools financial services organizations deploy? The data suggests that IT professionals believe easy-to-use tools that help users get their jobs done will ultimately improve security and compliance by keeping data on authorized applications.

The idea that users can have productivity or security is a false dichotomy. Today's financial services organizations are more connected with their customers, employees, and partners than ever. While these connections certainly introduce risk, they should also be embraced because of the benefits they can bring to the organization and its customers.

Far too many IT professionals in financial services lack trust

in their users to protect sensitive information, and too many users are relying on workarounds despite the importance the sector places on security and compliance. The path forward for addressing this issue requires an understanding of both the value and the risk of collaboration and connections.



An Endpoint-to-Endpoint Approach to Protecting Your Organization

BlackBerry® Cybersecurity Consulting can help you understand precisely where your organization's risks lie and support your organization in defining which business critical assets need protecting to help maximize the impact of your security investments and strategy. Instead of constantly reacting to the latest cybersecurity threats, BlackBerry will advise you on how to invest effectively in strategies to help future-proof your systems and organization. Whether you have an established cybersecurity approach and need to supplement, or you're starting to define it, BlackBerry Cybersecurity Consulting can help.

Following are some suggestions for financial services firms that find themselves in this situation:

- Recognize that human behavior (e.g., choosing the applications of least resistance) is difficult to change
- Understand that the use of workarounds represents the needs of users that are not being met by the applications currently available
- Address this risk with secure, easy-to-use applications that support collaboration and connectivity without introducing a burden on the users.

Future Technology Plans

The survey also asked respondents about their future plans for information technology. As a distributed ledger with a reputation for security, it's unsurprising that Blockchain is the emerging technology that the respondents believe will have the most impact on the financial services sector (Figure 5).

Please rank these emerging technologies according to the impact they will have on your industry.

Technology	1: Most Impact	2	3	4	5: Least Impact
Blockchain	37%	18%	16%	14%	15%
Quantum Computing – Quantum Safe Cryptography	23%	20%	18%	20%	18%
Machine Learning/ Artificial Intelligence	11%	31%	23%	23%	12%
Robots	15%	20%	37%	18%	10%
Intelligent Security	8%	16%	13%	33%	30%

Figure 5

Other emerging technology findings include:

- The emerging technology drawing the most interest among the surveyed IT professionals is voice technology (like Alexa or Google Voice). Nearly two-thirds (65 percent) of respondents say their organization has already implemented voice technology, and another 29 percent say they are reviewing or considering it.
- Slightly more than half (53 percent) of respondents say their financial services organization has IoT strategy in place.

On the surface, the adoption of emerging technologies like voice, IoT and AI seems like a solid strategy for improving business processes, customer experiences, and overall efficiency. Because many emerging technologies will also reduce the reliance on humans in some business processes – and the survey demonstrates that IT professionals in financial services lack confidence in their users' security practices – emerging technologies might also give the appearance of reducing risk.

In truth, the adoption of emerging technologies is likely to reduce risk in some areas while creating risk in others. In the same



way that human connections between employees, partners, customers, and distributors can increase risk, so too can technologies like IoT, which establish non-human connections that increase the attack surface.

The survey respondents seem to recognize the need for caution when they consider deploying emerging technologies. Their caution around voice technology might be a function of voice being the emerging technology most respondents are using or considering (Figure 6).

Which new technologies are you cautious about implementing?

Technology	Percent of respondents
Voice technology, Natural Language Processing	65%
Use of robots	40%
Intelligent security	37%
Quantum computing - quantum safe cryptography	28%
Machine Learning/Artificial Intelligence	26%
Blockchain	24%

Figure 6

Many of these technologies will help create new endpoints that operate largely without human interaction and often operate on the edge, beyond the traditional network. **This will require new approaches to security like chip-to-edge security, which creates trusted connections between fixed and mobile endpoints.** These trusted connections are essential to thwarting increasingly sophisticated attacks on increasingly distributed infrastructures.

“IT professionals believe easy-to-use tools that help users get their jobs done will ultimately improve security and compliance.”



BlackBerry Spark

BlackBerry® Spark is the only Enterprise of Things (EoT) platform designed and built for ultra-secure hyperconnectivity from the chip to the edge.

Key Takeaways from the Survey

- In the eyes of IT professionals in the financial services industry, users remain the weak point when it comes to meeting security and compliance standards. File sharing and mobility are areas of particular concern.
- Users find, and will continue to employ, workarounds if their needs are not being met. IT departments need to recognize user needs and embrace solutions that address them or they will continue to deal with the risks.
- Security and compliance need to be a more important consideration when researching and planning IT strategies in the financial services industry.
- IT organizations in financial services must take into consideration the adoption of applications that enable productivity and collaboration while also ensuring security and reducing risk of data leakage.
- Emerging technologies like IoT, AI, and more will introduce new risk because they increase the attack surface, and will thus require new approaches to security designed for this new paradigm.

BlackBerry can help balance your productivity needs with industry leading security

Nine of the top 10 global financial services brands rely on BlackBerry to connect their employees to the information they need, on the devices they want, with unparalleled security.

- Enable secure file sharing internally and externally, even after they leave your firewall
- Empower employees and consultants to use their own devices (Bring Your Own Device - BYOD)
- Secure mobile access to the apps your employees need
- Protect client data from hacks and reduce your liability
- Reduce risk, cost, and recovery time from ransomware attacks
- Comply with increasing regulatory requirements

To learn more about how BlackBerry secures the financial sector visit: <https://us.blackberry.com/enterprise/industries/financial-services>

About the Survey

The survey of 537 IT professionals in the financial services industry was commissioned by BlackBerry and conducted by QuinStreet, the publisher of eWEEK, eSecurityPlanet, and other websites for IT professionals. It was distributed via email to members of an independent, third-party panel in the United States, Canada, UK, Germany, France, and Switzerland between Nov. 28 and Dec. 5, 2018. The margin of error is +/- 4.5 percent at 95 percent confidence level.

“File sharing is a particularly vulnerable part of the security landscape in financial services.”