protiviti®
Face the Future with Confidence

Enhancing Security & Privacy in Financial Services Firms

Global cybersecurity risk has never been higher, yet its magnitude is almost certain to intensify in the months and years to come. Cybercriminal activity against global companies surged in the past year, with financial institutions continuing to be targeted for their high-value information. This makes cybersecurity a critical organizational priority and a top concern in the boardroom, C-suite and information technology function and in every area of the business for financial services firms.

It is imperative that boards of directors and executive leaders keep close attention on the state of their company's cybersecurity programs. Protiviti's 2017 Security and Privacy Survey delivers insights on the specific policies and qualities that distinguish top-performing companies from other organizations with regard to security and privacy practices. Although the responses from financial services respondents did not differ widely from the general survey, there are important nuances.[1]

Four Protiviti experts: managing director, Adam Hamm, former president of the National Association of Insurance Commissioners (NAIC) and former chairman of its Cybersecurity Task Force; Ed Page, leader of Protiviti's financial services industry technology consulting practice; Scott Laliberte, global leader of Protiviti's security and privacy solutions; and Andrew Retrum, managing director in Protiviti's financial services industry technology consulting practice, debate the financial services results from our latest Security and Privacy Survey. The results show cause for optimism but highlight consistent and growing concerns. Positive signs are particularly evident in financial services companies where the board of directors is highly engaged in information security matters and management has a robust set of key information security policies in place.

What are the top IT security and privacy-related challenges facing financial services firms today?

Andrew Retrum: There is heightened regulatory scrutiny around security and IT risk, as always, but firms are grappling with new, disruptive technologies, many of which are introducing new risks that are currently not being adequately managed. There is also the problem of shadow IT, IT systems and solutions built and used inside organizations without explicit organizational approval. Although most of our financial services clients would acknowledge that when they say they know where their crown jewels are, they are

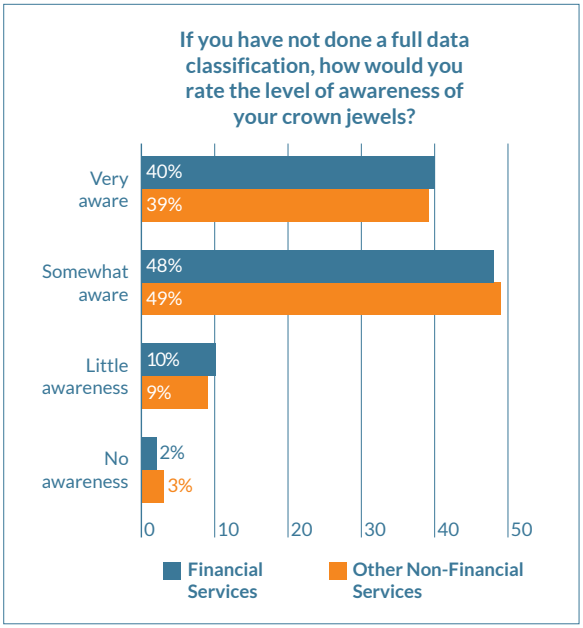
[1] See "Managing the Crown Jewels and Other Critical Data," Protiviti: www.protiviti.com/securitysurvey.

speaking from an enterprise-IT perspective and are not necessarily including all of the shadow IT applications or reports generated from end-user-developed or departmental systems that contain or impact the organization's crown jewels.

Scott Laliberte: Organizations need to understand regulatory expectations of third-party risk management and consider how they are managing their third-party vendors. In January, the National Institute of Standards and Technology (NIST) revised the NIST Cybersecurity Framework to include new details on recommendations for cyber supply chain risk management (SCRM), which is now a critical consideration in recognition of the fact that many organizations are outsourcing key business processes to, or sharing sensitive data with, third parties.[2] The U.S. Office of the Comptroller of the Currency (OCC) and other agencies have drafted regulations, titled Enhanced Cyber Risk Management Standards, addressing this "external dependency management."[3]

What more should firms be doing to identify and protect their crown jewels?

Ed Page: Financial institutions have millions and millions of data elements, which are of varying importance to different areas of the business. Firms need to be able to categorize their data to distinguish the criticality of various data elements. Because they cannot effectively control everything, they need to ensure they are controlling the right things. For years we have talked about the importance of data classification and making sure firms understand the relative importance of sensitivity of data. If that isn't done effectively, it is impossible to know where to focus the attention.



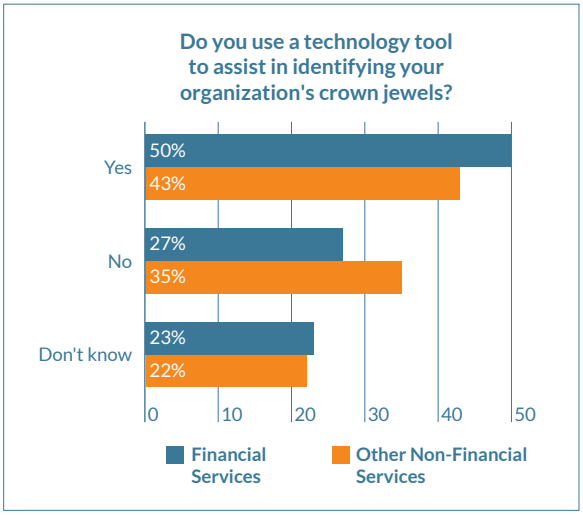
Laliberte: To be able to effectively protect sensitive data, it is not enough to identify the organization's crown jewels and put in place defense systems. Firms need to focus on how they are segmenting data so that, in the event of a breach, the bad actors aren't able to access all of the crown jewels at the same time.

Adam Hamm: Regulators expect companies to protect non-public information (NPI) and personally identifiably information (PII) to the greatest extent possible because that data is most easily used to perpetrate fraud. On top of that, companies are expected to protect their business data in general but the foremost priority is to protect the personal information of their customers. Performing a risk assessment, as required of firms in New York State under the New York Department of Financial Services cybersecurity regulations, for example, allows firms to identify that data and where it resides within the organization.

[2] "Cybersecurity Framework Draft Version 1.1," *NIST*, January 2017: www.nist.gov/cyberframework/draft-version-11.

[3] "Enhanced Cyber Risk Management Standards," OCC, Federal Reserve, FDIC: www.occ.gov/news-issuances/news-releases/2016/nr-ia-2016-131a.pdf.

Most firms use a technology tool to assist in identifying their crown jewels. Are such tools necessary, and how do they help?



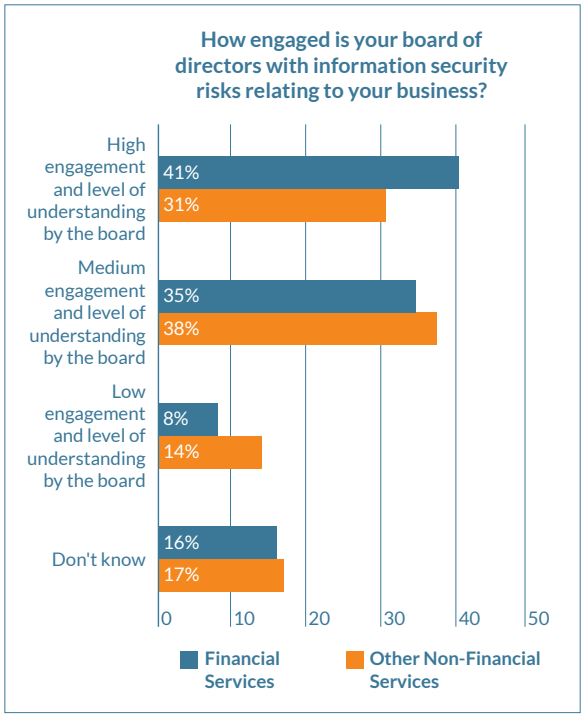
Retrum: Firms need to leverage tools to identify their crown jewels; manually, identification is resource-intensive, often inaccurate and prone to error. There are many tools that can assist this process, from those that perform data discovery checks to those that monitor traffic to help identify where the crown jewels are at rest and where they are moving to throughout the environment and beyond. The sheer volume of data that firms collect necessitates the use of management tools.

Page: All financial services firms should be leveraging some kind of tool to understand or help identify where that sensitive information lies within their environment. But this is not the only concern; firms also need to consider the implication of data that is stored outside of the organization's virtual walls with third-party vendors or SaaS providers, for example.

Boards of directors of financial firms are more engaged and have a higher understanding of information security risks affecting their business compared to other industries. What does this tell you about the level of board engagement at financial institutions?

Hamm: Financial institutions are being attacked and breached more often than other parts of the economy due to the high value of their information. This has raised the issue to the board of directors' attention and involvement, in part because they need to be engaged as part of their board duty of care in the event there are any lawsuits against the company relating to a breach.

Retrum: Two of the top five risks in Protiviti's annual top risks survey were IT security or cyber related.[4] Once these risks appear in the lists of top risks, they attract executive leadership and board visibility, as well as closer regulatory attention. The National Association of Corporate Directors (NACD) is highlighting cyber risk much more so than in the past and issued a revision edition of the NACD *Director's Handbook on Cyber-Risk Oversight* in January 2017.[5]



[4] See *Executive Perspectives on Top Risks for 2017*, North Carolina State University's ERM Initiative and Protiviti, www.protiviti.com/toprisks.

[5] *NACD Director's Handbook on Cyber-Risk Oversight, NACD and ISA, January 2017*: www.nacdonline.org/Cyber.

Laliberte: Board awareness in financial institutions is being driven by regulatory guidance. The Gramm-Leach-Bliley Act (GLBA) Section 501(b), as well as guidance from the Federal Financial Institutions Examination Council (FFIEC), both refer to regular cyber risk reporting to the board and management — all of this is pushing boards to become more aware and involved in cyber risk management.

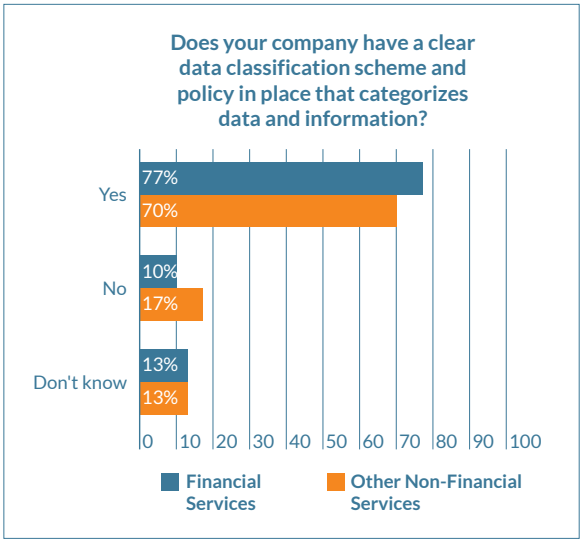
Over half of financial services respondents to the survey said that there were "moderately confident" they could prevent a targeted external attack by a well-funded attacker. Is this an accurate assessment of most financial institutions?

Laliberte: Given the current environment, I would not expect any firm to have a high degree of confidence — or even to be moderately confident — that it could defend against a well-funded attack. These results may reflect a measure of false confidence at some organizations.

Page: It is not a matter of if an organization will be target, it is a matter of when. The onus on firms is to ensure they are protected to the best of their ability but to also prepare for how to limit the impact of an attack.

Although more financial services firms say they have a clear data classification scheme and policy in place compared to other industries, given the sensitivity of financial information, would you expect the difference to be more pronounced?

Page: The financial services industry has been discussing and performing data classification projects and has had a strong focus on data governance for more than a decade, and as a result, most firms have mature data classification and governance programs in place. However, the complexity of the infrastructure makes this a difficult task, so it is not surprising that this is still a challenge for some firms.



Retrum: The results show that financial services institutions are more self-aware of the data problem and are subject to higher data governance standards than some other industries.

According to the survey, financial services employees understand the need to differentiate between public and sensitive data from acquisition to destruction. Can this be explained by regulation alone?

Hamm: It is not only regulation; the high-profile breaches and their aftermath, including the potential for lawsuits, is driving firms to better manage their data to better protect themselves.

Laliberte: Companies are very aware of the lawsuits and fines levied by the Consumer Financial Protection Bureau (CFPB), but the regulators constantly reinforce this predicament for financial services firms. Other industries are much less mature. Healthcare, for example, is a highly regulated industry, but the regulators have far less power, so fewer actions are being taken. Financial institutions were hit hard by the CFPB fines and other regulatory actions that acted as a catalyst for change.

Although all firms have a crisis response plan in place, the quality and understanding of such plans by senior management varies. Should firms be performing more tests?

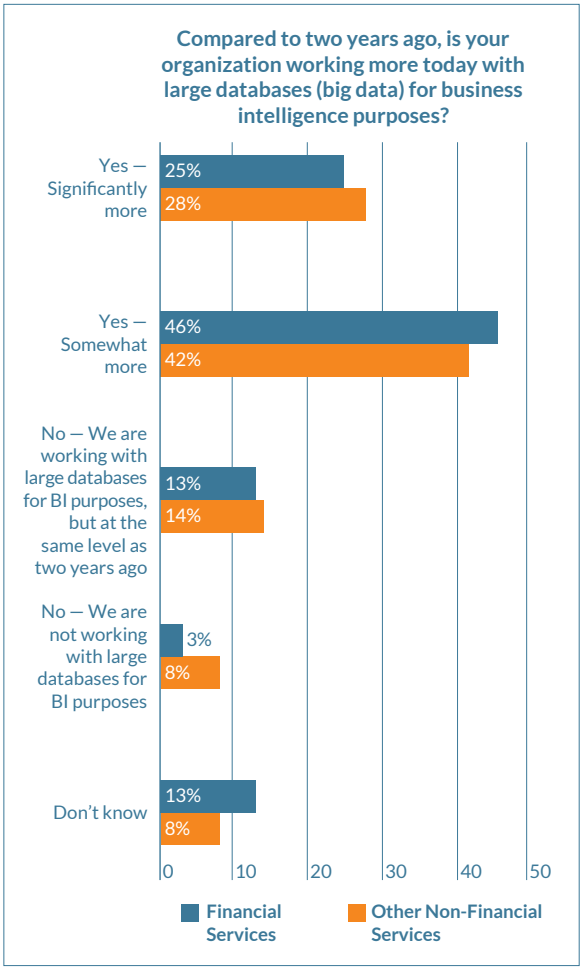
Hamm: There are currently no specific requirements for testing crisis response plans. Regulators strongly believe an incident response plan is critical, but they do not go into detail about how they should be tested.

Retrum: This question is gaining traction in the industry, and we are receiving more inquiries about the need to perform large-scale scenario-based exercises, which may indicate the beginning of regulatory attention in this area.

Page: Tabletop exercises are useful for developing and assessing crisis response plans, and they help firms cover a lot of different scenarios that are more than just cyber risk, such as natural disasters, for example, but they are just one tool and are certainly insufficient by themselves. Firms should understand their risk appetite, then design and execute tests that reflect that.

Most financial services respondents indicated that they were working with more big data for business intelligence compared to last year. What should firms be concerned about with regard to their growing use of big data?

Page: One of the big problems with big data is the data classification issue. Big data includes structured and unstructured data, which is more difficult to classify. Similarly, firms may also be dealing with new technologies with different security characteristics and maturity levels, as well as more data being distributed into the cloud. All of these factors are complicating data management for financial institutions.



Laliberte: As previously mentioned, understanding what data is critical to protect, its location and its journey throughout the lifecycle is essential. The use of big data complicates this further, especially as there may be many more people interacting with it and manipulating it. Firms need to make sure they are controlling access to that data.

Hamm: An added consideration is that firms need to have a complete understanding of what they want to use certain information for so they can assess if any channels are currently or potentially disallowed by regulators. Geolocation data, for example, is currently

used by many firms, but it is on the regulatory horizon regarding privacy laws. This whole area of big data is something that regulators are getting involved in more and more, in terms of what they are going to allow companies to use and how they will be allowed to use it. Companies should be concerned about getting too far ahead of their regulators in this area.

The use of cloud computing is growing among financial institutions. What should firms be considering to ensure that security is being addressed, and what are the implications for vendor management?

Page: Less than two years ago, the financial services industry was considered to be a bit of a laggard in terms of cloud adoption, but as our survey data shows, this has changed significantly as institutions have become more comfortable with the cloud. This is a reflection of the improvement in cloud security capabilities as they have matured, but firms still need to ensure they are diligently applying security policies and procedures.

Hamm: It is too early for any regulatory guidance around the use of cloud services, but from a third-party risk management perspective, firms need to ensure they are complying with all existing requirements around security and risk, which can be proven during an examination.

More and more firms are using third parties to access better services and more advanced technology, but are financial institutions doing enough to counter new risks, such as partnerships with fintech companies?

Page: The reality is that financial institutions are digital businesses, with more and more capabilities being provided via mobile devices and embedded in other firms' services. Traditional financial firms are partnering with financial technology, or fintech, companies, many of which are small start-up organizations that may not have the same rigor or discipline as financial services firms typically have. While this is necessary to compete in today's fast-paced world, organizations need to acknowledge this situation and take appropriate steps to be diligent about how the parties interact.

Laliberte: Third-party risk management continues to be a challenge.[6] Although financial services companies are ahead, there remains much maturing to be done in this area. For example, many institutions are using their own methodologies and their own questionnaires to assess third-party risk, which creates a lot of confusion in that whole industry. One third-party provider could be working with 50 different financial institutions and receive 50 different questionnaires and audits throughout the year, draining resources. They would love to have a more definitive standard and benchmark assessment process to provide comfort to their financial institutions partners, and vice versa.

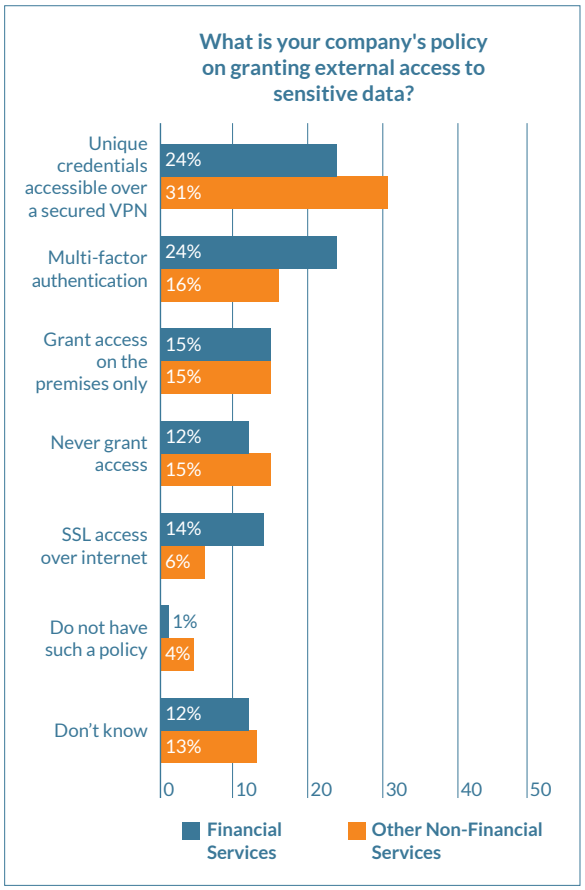
Retrum: Many third-party assessments tend to be very much inquiry- and paper-driven, and do not necessarily test key controls. Financial institutions need to ensure those controls are in place to minimize the risk from third parties. For instance, if you have third parties that need access to certain technologies or data using BDI technology with multi-factor authentication where that third party is accessing it securely, firms can ensure the data never leaves the facility.

Only 24 percent of financial services respondents state that they have a multi-factor identification policy on granting external access to sensitive data. What more should firms be doing to better protect their data?

Hamm: In the insurance industry, this is one of the issues where the industry pushed back hard against the regulators, whose default position is for firms to have multi-factor identification in place.

[6] For more information, read the *2016 Vendor Risk Management Benchmark Study*, Shared Assessments Program and Protiviti, available at www.protiviti.com/vendor-risk.

The industry, however, cites countless reasons why it is not necessary, primarily the low return on investment. If the regulators aren't going to require multi-factor security in insurance, at least, the industry response will be much more varied. But firms should be looking at multi-step and other methods to reduce the risk exposure of unauthorized people getting access to personal data.



Laliberte: The FFIEC issued multi-factor authentication guidance back in 2005, which stated that firms need to perform risk assessments and consider multi-factor access for any high-risk transactions. What constitutes high risk, however, is left open to subjectivity and has resulted in many organizations taking advantage of that freedom. In general, given the sensitivity of information financial services hold and the focus of the regulators, I would have expected this statistic to be higher.

Page: Having worked in the financial sector, I have seen firsthand the incredible push and pull between ensuring ease of access and making it simple for customers and their employees to do their work and security. This remains a raging debate within a lot of organizations. It will be interesting to see how this debate evolves over time and whether or not emerging and evolving multi-factor authentication capabilities can solve for both security and ease of use. Biometrics and behavioral analytics, for example, may be options to eliminate passwords and user IDs, yet allow for layering security in an effective manner.

Hamm: The New York Department of Financial Services cybersecurity regulations cover a broad range of topics, including multi-factor identification, incident response plans and cybersecurity policies, which all flow from the risk assessment component of the regulations.[7] Every regulated entity is expected to perform and document an enterprisewide risk assessment to identify their cyber vulnerabilities, which will inform the cybersecurity program and policies they need to have in place and how they need to approach multi-factor authentication, encryption and incident response plans. Other regulators are likely to introduce similar cybersecurity regulations that will predictably start with that all-important risk assessment piece to discover where improvements need to be made.

IT security and privacy reporting lines are varied at financial institutions. What are the pros and cons of the different reporting lines for security and privacy matters?

Page: Chief risk officers were not included as an option in our survey, but we are starting to see some shift in financial services towards security teams reporting to the CRO. There is a definite shift away from security and privacy remaining embedded in IT, although that remains the case in many organizations.

[7] See Protiviti Flash Report, "New York State Proposes New Cybersecurity Regulations" www.protiviti.com/sites/default/files/united_states/insights/protiviti-flash-report-ny-cybersecurity-regulation-092016.pdf; and "New York Steps Up With First State-Level Cybersecurity Regulations for Financial Services Companies" https://blog.protiviti.com/tag/nydfs-regulation/.

Hamm: There are pros and cons of both options, but from a separation-of-duties perspective, it makes sense for the reporting line to go up to the CRO, because security is not just about technology. There is a very strong argument to be made that it belongs somewhere else, either with the risk function or elsewhere. The other side of the argument, however, is if there is a ton of technology that needs to be deployed that will affect security, the engineering and technical responsibilities arguably should remain with IT. If the reporting line does gets moved, careful coordination with IT needs to remain. There is a price to be paid for moving the reporting line, but that separation-of-duties aspect is a strong argument for moving it to the risk function.

Laliberte: A hybrid reporting line is possible. Firms can have operational security processes and responsibilities embedded in the IT organization with the more governance, oversight and risk management elements of security, which belong to risk or another function, with the proper separation of duties.

Contacts

Ed Page
Managing Director
+1.312.476.6093
ed.page@protiviti.com

Scott Laliberte
Managing Director
+1.267.256.8825
scott.laliberte@protiviti.com

Adam Hamm
Managing Director
+1.312.476.6334
adam.hamm@protiviti.com

Andrew Retrum
Managing Director
+1.312.476.6353
andrew.retrum@protiviti.com