Real Time Research REPORTS

silo By Authentic8

Surprising Disconnect Over Compliance and Secure Web Use at Financial Firms

Why Compliance, IT and Legal Must Restore Trust and Get Into Sync

Surprising Disconnect Over Compliance and Secure Web Use at Financial Firms

Why Compliance, IT and Legal Must Restore Trust and Get Into Sync

Executive Summary

The legal, compliance and IT departments at financial firms frequently have strikingly different priorities when addressing security and compliance issues. This disconnect creates the potential for sizable gaps in compliance and data protection approaches in these organizations if they are not properly and jointly addressed by the Chief Risk Officer (CRO), Chief Compliance Officer (CCO), and Chief Information Security Officer (CISO).

To deal with the situation, leading financial companies are beginning to implement shared strategies that work well for all three departments. The hallmarks for success include a focus on monitoring employees' online behavior; regular evaluation of governance and compliance processes; and use of proven technologies such as activity monitoring and remote browser isolation to maximize security without burdensome restrictions on employees.

Key Findings for Compliance and IT Security Leaders

Financial firms with a lower ratio of IT personnel to overall workers are more acutely aware of financial and security risks.

- Compliance teams are more apt to focus on reducing malware incidents and closing security/compliance gaps caused by employees' access to social media sites than legal and IT.
- IT departments involved in compliance efforts from the outset are more likely to be receptive to new approaches besides relying on solutions already in place.
- Organizations must work harder to overcome their departmental disconnects and to develop clear strategies to secure data without creating an onerous situation for workers.

Introduction: How Fragmented Perspectives Increase Risk

Financial firms have some of the best-funded IT departments of any industry. Nonetheless, compliance, legal and IT security departments often have different takes on how to handle data security and regulatory matters, creating a divide that can lead to security and compliance issues.

This is one of the key findings of a survey of more than 160 financial institutions and law firms serving the financial services industry that was conducted in the summer of 2019 on behalf of Authentic8 in association with Beacon Technology Partners and Triangle Realtime Reports. The survey involved senior decision-makers in IT, legal and compliance roles. (For additional information about the methodology and demographics, see methodology on page 13.)

"These three groups are working on the same problem, but they have different views of what the main problem is," says Michele DeStefano, a law professor and co-founder and co-editor of the Compliance Elliance Journal. "When you have three different groups solving for different problems, that's when you find gaps."

While the potential for disconnect worries experts, the study also shows a clear strategy is emerging for how leading financial firms can secure their data and ensure regulatory compliance without creating an undue burden on workers. This report explores the survey findings, as well as the steps financial and legal organizations can take to safeguard information today and in the future.

How Resources Shape Risk Perception

Many factors can affect a company's concerns about data vulnerability, including the extent of a company's IT resources. The survey discovered financial companies of all sizes that have a lower ratio of IT personnel to serve the employee population—what might be described as "less accessible" IT departments—are more acutely aware of the risks and the time it takes to diagnose and remediate the aftereffects. Large organizations with many field offices often fall into this category of "less accessible" departments.

The survey shows that 57% of these "less accessible" IT departments are concerned about unauthorized access and intrusion. In addition, 50% are worried about web-borne exploits and attacks; 50% about the lateral spread of malware; and 50% about blended threats and multi-pronged attacks. Some 44% are concerned about denial of service attacks. In each case, these concerns are significantly greater at companies where IT resources are spread thin. [See Figure 1]

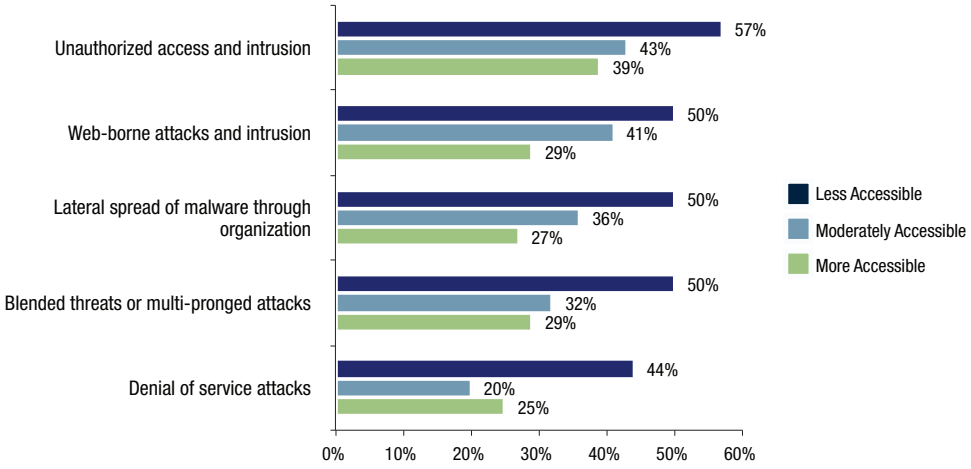
Feeling Vulnerable

IT departments with fewer resources per employee ("less accessible") are more concerned about attacks.

How concerned is your organization with the following types of attacks which may impact its data and systems?

"CONCERNED" SUMMARY—(TOP 2 BOXES, 7 PT. SCALE)

FIGURE 1



In addition, these "less accessible" IT departments feel significantly more challenged by potential data loss, preventing malicious text messages, and enabling remote access by employees and external contractors. Maintaining operational security in research and investigations is another top concern. [Figure 2]

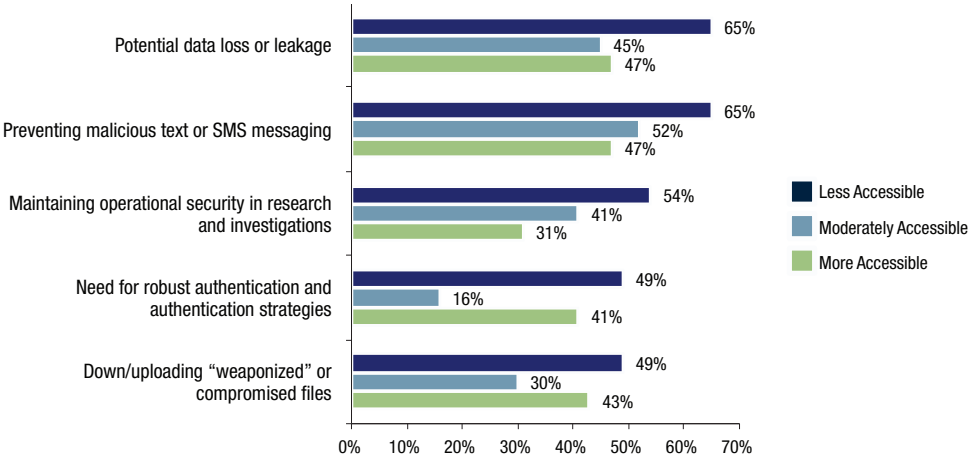
More Challenges for Less-Accessible IT Teams

Protection against data loss and malicious messages seen as biggest challenge.

How challenging are the following IT security concerns?

"CHALLENGING" SUMMARY

FIGURE 2



The IT head at one financial firm we interviewed, where roughly 20% of the total 50 employees are in the technology department, provided the backdrop for these concerns. "You need to have a certain critical mass of IT employees to run your operations in an efficient way," he explains. "However, I know peers who work at similar sized companies as mine where the IT department is only one person. The ratio of IT employee to total employee population really matters. The IT person has so many things to do that it's hard to do any of them well."

"Less accessible" IT departments are looking for ways to be proactive, according to the survey. For example, they want their people to be able to do things like check their LinkedIn profiles or their personal web-based email in a safe and not overly restrictive way. But even those with more accessible IT staff support find that real time monitoring of online behavior and user provisioning can be difficult.

The IT head of the 50-person financial firm explains that many employees work long past standard business hours advising clients. "To tell them that they can't access their personal email while sitting in the office is a huge burden on them," the IT director says. "But having them use their browsers and open web mail attachments was too much of a risk for me. That put us at a bit of a crossroads. I was enforcing policies and the users weren't happy."

Disparate Perspectives Without Alignment = Increased Risk

While IT, Legal and Compliance are all concerned about security, they differ as to which risks are most pressing. "Their ultimate goals are the same, but their focus is different," says Michael Osterman, president of Osterman Research, a market research and consulting firm focused on the messaging, collaboration and web industries. "They understand that they look at things differently, but they don't truly appreciate the issues that the other departments face. Compliance doesn't realize how difficult it is for IT to get things up and running, and how many users are doing dumb things that put the company's data at risk."

Our survey provided a clear lens on those different ways of thinking. Compliance teams are more apt to focus on reducing malware incidents and closing security/compliance gaps caused by employee access to social media sites. While these issues are acknowledged by legal and IT, they are uppermost on the minds of the compliance team. [Figure 3]

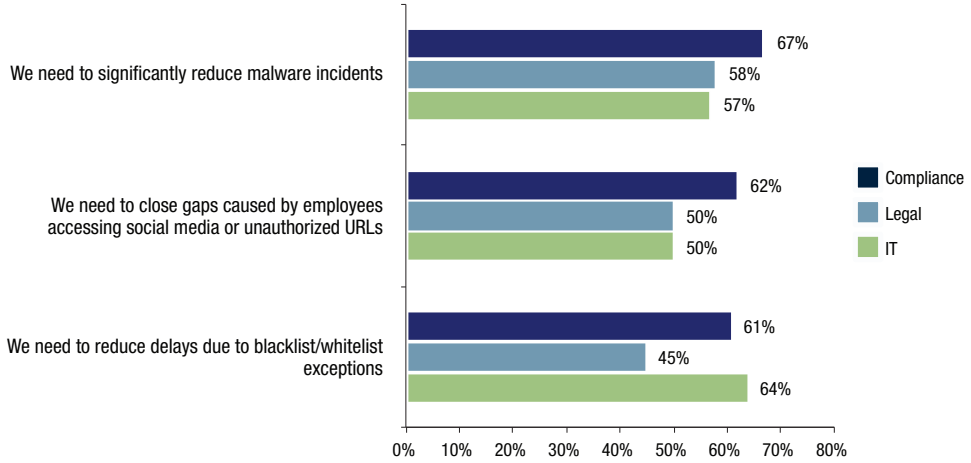
Compliance Teams Focus on Reducing Risks

Chief concerns of compliance teams are reducing malware and securing social media.

Please tell us whether you agree or disagree with each of the following statements regarding IT security procedures and solutions.

"AGREE" SUMMARY (TOP 2 BOXES, 5 PT. SCALE)

FIGURE 3



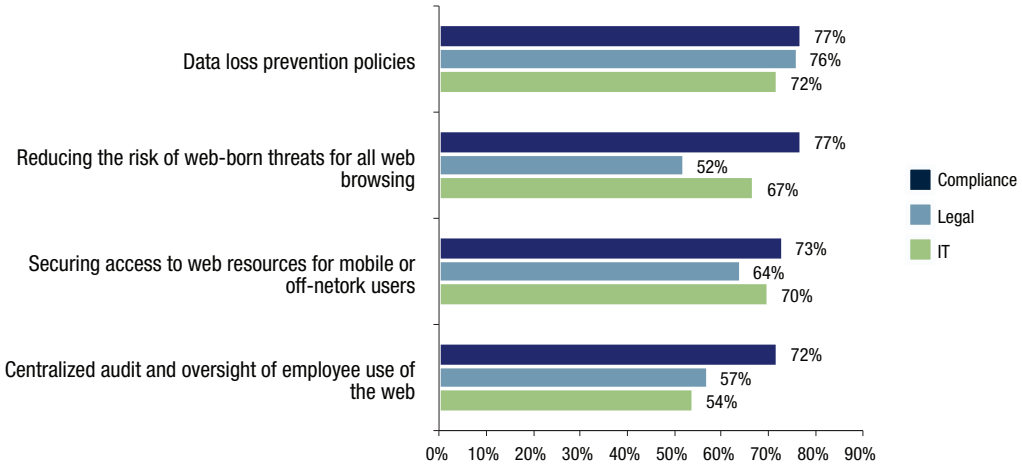
Legal departments, in contrast, are more concerned about setting data loss prevention policies and reducing the risk of web browsing, as well as securing access to web resources for mobile users. Moreover, legal departments are highly attuned to IT security policies, such as centralized audits and oversight of employee web use. While security policies are also important to IT, it's possible that IT workers have developed some "tunnel vision" where they focus more on traditional perimeter defenses and point solutions. [Figure 4]

Legal Relies on Security Policies

Legal departments are particularly attuned to IT security policies.

Which of the following IT security policies or objectives has your organization instituted?

FIGURE 4



Meanwhile, IT is more deeply concerned about potential attacks than their colleagues in compliance and legal departments, as well as about pushback from employees for restrictive policies. "The typical IT department is overworked and stressed," Osterman says. "There's a lot on their plate. Their focus is on managing the infrastructure and dealing with user complaints." [Figure 5 and 6]

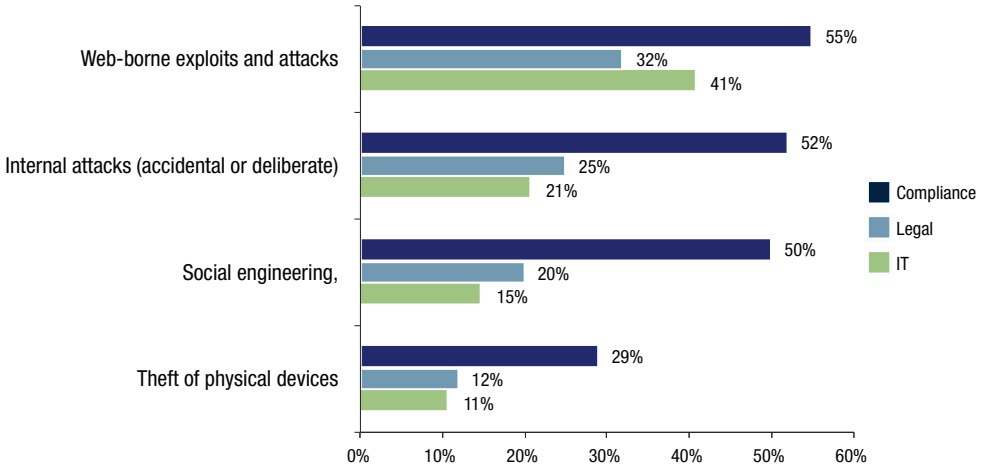
IT Remains More Attuned To Potential Attack Vectors. . .

IT departments are more aware of how attacks can happen than other departments.

How concerned is your organization with the following types of attacks that may impact its IT data and systems?

"CONCERNED" SUMMARY (TOP 2 BOXES, 7 PT. SCALE)

FIGURE 5



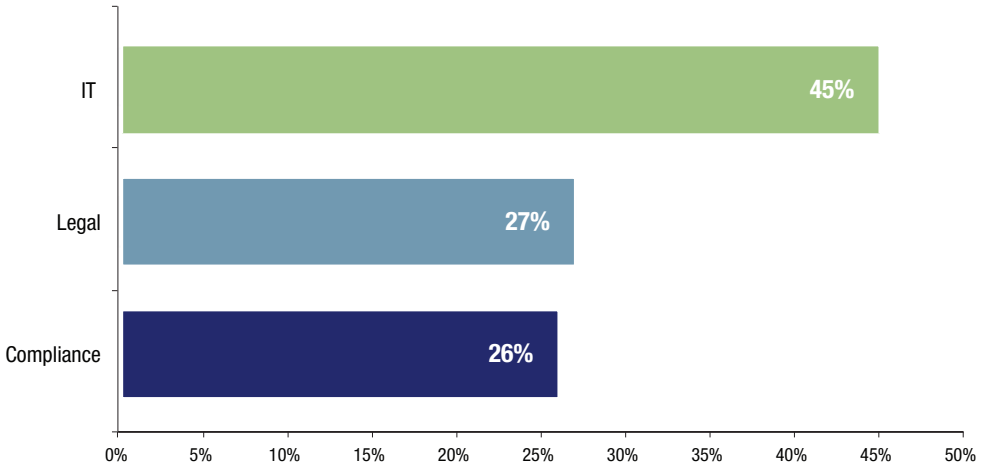
. . .and Pushback From Users

IT is sensitive to employee complaints about overly restrictive security policies.

Do you agree or disagree that users are unhappy with your IT security procedures?

"AGREE" SUMMARY (TOP 2 BOXES, 5 PT. SCALE)

FIGURE 6



While the differences are understandable, they also suggest the three departments may all be putting too narrow of a lens on a complex problem.

Action Item

To overcome compartmentalization and reactive approach, convene a regular Data Protection and Compliance brain trust to advise the CEO or Chief Risk Officer.

"Companies are seeing a disconnect as they try to deal with digital transformation, ask legal departments to be leaner, and face tightened rules about cybersecurity and information sharing," DeStefano says. "It keeps me up at night knowing these three groups are working on the same problems but not really collaborating closely enough to solve them."

The survey findings suggest clear lines of responsibilities among the three departments. In many companies, Legal is leading the charge in raising the issue with top management. Compliance is more involved in setting the tone for how financial services should approach these issues. Meanwhile, IT remains the most acutely aware of the vulnerabilities, overhead and resource issues—and remains most sensitive to user feedback.

"IT is focused on minimizing the number of moving parts, while compliance and legal are focused on making sure nothing breaks," Osterman says, "The friction between the departments can lead to data loss."

Some experts believe companies would be better served by making entities more equal partners rather than segmenting their responsibilities so narrowly.

"Going forward many sophisticated companies will ostensibly become technology companies," explains Tom C.W. Lin, a professor at Temple University Beasley School of Law, whose research focuses on financial technology, financial regulation and compliance. "IT and compliance departments will have to work together in a more intertwined fashion where IT and compliance functions become one deeply, coordinated and extricable core function of a business."

How to Leverage the Web While Maximizing Security

A primary issue in safeguarding data is controlling the time and access that employees have to the internet, while using corporate resources responsibly. "One of the most challenging issues for businesses in this area is balancing concerns about cybersecurity caused by employees with the need to provide employees with the freedom to be autonomous, creative and productive," Lin says.

Companies with "less accessible" IT want to enable remote access, centralized management and robust user activity monitoring. The survey found remote browser isolation, user behavior monitoring

online, and governance risk management and compliance (GRC) were the top three IT security considerations in the financial industry. Each of these is embraced by more than four out of every 10 firms. User behavior analytics—the tracking, collecting and assessing of user data and activities using monitoring systems—was ranked as the top total opportunity for IT security solutions in the survey.

Action Item

Identify solutions that allow for direct visibility into employee online activities in real-time.

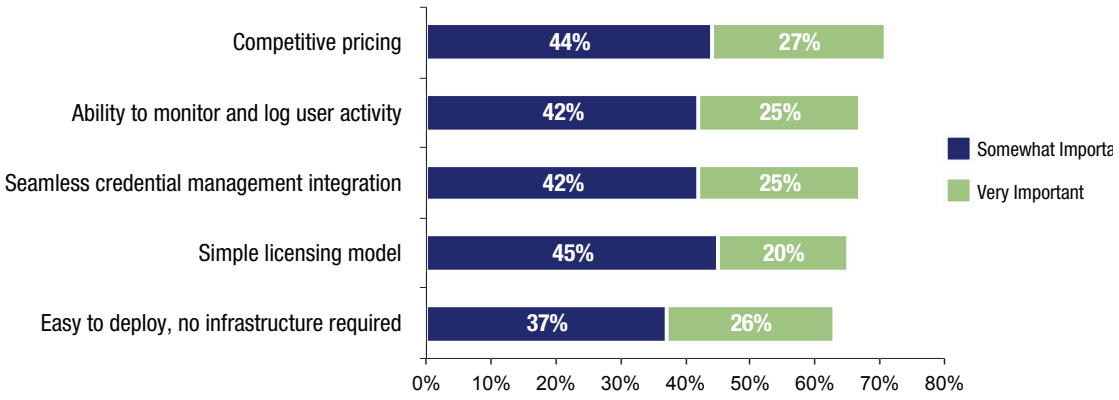
Companies are also clear about what attributes they expect from each of these technologies. While competitive pricing tops the list, other key factors that organizations prize are ease of use and the ability to monitor and log user activity. Both attributes were considered very or somewhat important by more than 60% of the surveyed companies. [Figure 7]

Activity Monitoring Capabilities Rank High

Ease of deployment is universally important.

When your organization chooses to adopt IT security policies and solutions, how important are each of the following factors?

FIGURE 7



Given the onslaught of cyber attacks, and how insidious they have become, IT leaders feel monitoring technology is essential to keeping ahead of potential threats.

Ongoing evaluation of risk, compliance and governance operations was the second-highest ranked security process in the survey. For example, one IT person we spoke to who is assigned to the legal department of a leading financial services provider sat down with lawyers and crafted a 45-page governance document about what actions his fraud-detection team could take to minimize risks. The IT person continues to meet with the lawyers on a quarterly basis to help them understand the nuances of battling fraud.

"The lawyers don't understand that the social platforms they are used to in the United States aren't the same ones that are used in Russia and Latin America," he says. "Since we are an international operation, we need to help Legal understand how quickly things change. And my team needs to understand how the regulations and statutes are changing, so we can ensure we are operating in an effective, ethical manner. We want to make sure we do nothing that would wind up in a courtroom or on the front page of the *Wall Street Journal*."

Remote browser isolation was the third key strategy among the most valuable security solutions in the financial industry. With traditional browsers, every time an employee views a web page, potentially harmful code from the internet enters the corporate network and executes on the endpoint. This poses the risk of malicious code, such as ransomware, spyware or malvertising, infecting the firm's network and creating significant financial and reputational damages as a result.

Browser isolation is a cybersecurity model used to physically isolate an internet user's web browser and browsing activity away from the local machine and network. It is the underlying model and technology that supports a remote browsing platform. It is designed to:

1. Strengthen and simplify the security architectures;
2. add control over sensitive data, apps and workflows; and
3. give users secure web access and the ability to conduct critical web research.

This approach is already changing how the industry is conducting sensitive and compliance-relevant research, as the interviews for this report indicate. One example was described by the head of fraud investigations for a global financial firm. His team uses cloud-based browser isolation to safely investigate sites based in foreign countries and on the dark web. "We have to make sure the identity of the analysts and the company are protected," he says.

The IT director of the 50-person financial services firm emphasized in the interview how browser isolation also enabled his firm to provide employees with access to the web to attend to personal matters when necessary, without sacrificing security or compliance. In an industry where working around the clock is standard, trying to bar external web access proved untenable.

"It was very painful to tell people they couldn't check their personal email on company technology," he says. "In our industry, everyone is so busy that you have to run your personal life from the office. Browser isolation was huge for us and solved the problem."

Across the financial industry, consensus is building that robust user behavior monitoring and remote browser isolation—together with better compliance and identity management tools—are critical IT security components in ensuring secure and compliant access to web resources. Overall, companies agree they need a solution that provides easy and compliance-friendly logging and auditing for real-

time visibility into employees' online activities and creates an isolation layer between the user and the web that is effective, affordable, requires minimal maintenance and remains transparent to the end user. [Figure 8]

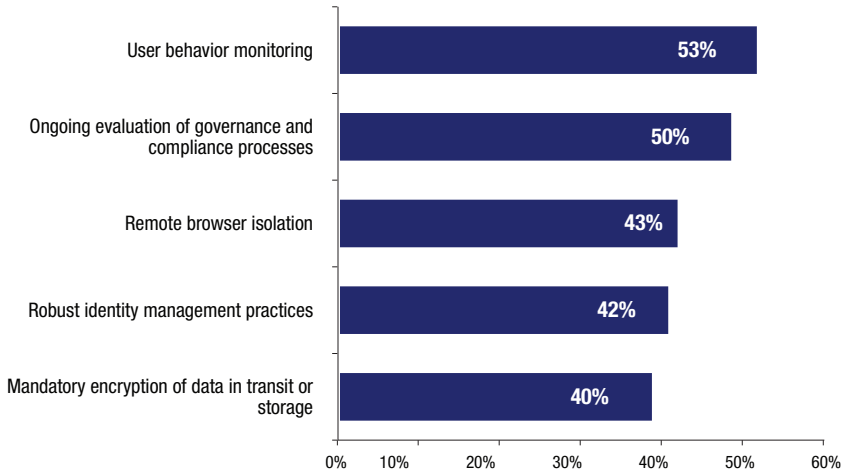
Protection Strategy Emerging

Companies are focusing their technical resources on monitoring their employees' online activities, governance and remote browser isolation.

Which of the following IT security processes or applications does your organization currently use, deploy or is considering in the next two years?

IT SECURITY PROCESS / APPLICATION STATUS (TOP 3 BOXES: INTERESTED/CONSIDERING, LOOKING, OR NEED MORE INFO)

FIGURE 8



Summary: How to Overcome the Disconnects

Financial companies, more than other industries, are finely tuned to the risks of data loss and the need for better security. Solutions that address the different concerns and priorities from Legal, IT and Compliance will need to be balanced, while also create a satisfactory work climate that restores trust and allows safe and acceptable browsing.

Three approaches are considered particularly useful for both small and large organizations with "less accessible" IT departments already struggling to handle day-to-day chores:

- Automating processes;
- providing secure access to the web; and
- centrally managing and monitoring web, social media and cloud app usage to ensure compliance.

Each approach can help overcome security deficits compounded by a lack of staff. As financial firms look to the long-term, they should also consider closing the awareness gaps that exist among IT, compliance and legal teams when it comes to heightened security risks and listen to users who want a higher degree of work/life balance.

Action Item

Involve IT in compliance efforts from the outset to maximize security and compliance and avoid papering over ineffective solutions already in place.

"Compliance shouldn't be separate from legal, because then you are separating the why you're doing something from the what we're doing and how we're doing it," DeStefano says. "Financial firms should move to a flatter organizational structure between those groups. IT should be involved in the beginning rather than at the end."

Methodology and Participant Profile

A total of 163 respondents completed the survey from May 23 to July 19, 2019. Only financial services companies and law firms with clients in the financial services industry were able to complete the survey. Job responsibility included senior level compliance officers (with 61 completes); legal managers (with 60 completes); and IT management (with 42 completes). All respondents identified themselves as personally involved in setting policies and procedures for managing security of IT operations, infrastructure and regulatory compliance for their organizations.

Sponsor Perspective

How to Maximize Security and Compliance with a Centrally Managed Cloud Browser

Web browsers were designed in the 1990s, as a tool to request page data from remote hosts and arbitrarily execute the payload. As the web has increased in sophistication and reach, the browser's architecture has become a liability, resulting in data breaches, malware attacks and compliance violations.

The tight interdependency between the browser, plugins, and the local operating system and its resources allow for the execution of arbitrary code that threatens the local device, network resources, and data. The basic interaction model of the web has created an environment where a simple page view request can lead to system exploits and data egress.

The architecture of the web is too entrenched, the execution model won't change. Instead changing the location of the browser creates a security layer without requiring a change to the underlying technologies.

A browser built in the cloud, executing all web code remotely, enables financial firms to maximize security and compliance when employees and contractors access the web. With browser isolation in the cloud, as pioneered by Authentic8, the attack surface shifts from the local IT infrastructure to a secure cloud container.

Each session is built on a fresh instance of the Silo Cloud Browser. No web code ever reaches the device, and no cookies, trackers, or other cached data persist across sessions. The browser executes everything on a remote host configured for security and regulatory compliance.

As code is rendered in the isolated environment, authorized content is converted to an encrypted and interactive display of the page and delivered to the endpoint device over an alternate, non-HTTP protocol. Users enjoy full-fidelity access to web content with no risk.

The cloud browser model also makes it easy to meet and monitor regulatory compliance requirements because it enables IT to centrally manage credentials, permissions and policies:

- Admins can enforce access and use policies, to ensure compliant access to the web and authorized use of cloud apps
- While conducting research online, analysts and fraud or AML investigators remain completely anonymous and insulated from web exploits.
- Encrypted, verbose audit logs allow for internal oversight of employee activities online and support compliance and remediation requirements.

Silo insulates employees from all web-borne threats to ensure security and good governance. Centrally managed, compliance-ready and audit-friendly, Silo provides fast and secure access to the parts of the web that are essential for running a productive and competitive business.

SCOTT PETRY
Co-founder and CEO
Authentic8, Inc.

TO LEARN MORE, VISIT: www.authentic8.com/silo

Real Time Research REPORTS

Silo By Authentic8

TO LEARN MORE, VISIT: www.authentic8.com/silo