Bloomberg Law

Professional Perspective

Adjusting Information Security for Long-Term Telework

Amanda R. Lawrence, Elizabeth E. McGinn, and James C. Chou, Buckley

Adjusting Information Security for Long-Term Telework

Contributed by Amanda R. Lawrence, Elizabeth E. McGinn, and James C. Chou, Buckley

Amid a fast-moving pandemic in the spring of 2020, many companies were forced to adopt remote-work operations almost overnight to maintain critical business functions. This approach initially seemed like a temporary and imperfect solution to maintaining workforce safety while continuing essential operations.

The solution no longer seems fleeting, however, as companies increasingly recognize the benefits of telework. But expanded remote working elevates a range of cybersecurity and information security risks that companies must address if it is to be part of a longer-term strategy.

Institutionalizing remote-work operations can result in enhanced productivity, resiliency, and workforce flexibility. However, remote-access capabilities will also require focusing attention on the company's information security program, particularly with respect to risk assessments, applicable classification and access control policies and standards, device management, unique information security risks associated with the use of cloud service providers, and cyber insurance coverage.

Federal agencies, including the National Institute of Standards and Technology and the Cybersecurity and Infrastructure Agency, have issued broad guidance that outlines baseline security measures for remote work, and primarily focuses on rapid solutions to protect the confidentiality, integrity, and availability of company information. These include the following recommendations:

- Expanding data backup, recovery, and resiliency programs
- Using strong authentication protocols, such as multi-factor authentication, and establishing role-based access controls
- Implementing endpoint security for email, applications, mobile and storage devices, and networks, such as anti-virus/malware, firewalls, log monitoring, and other intrusion detection devices
- Securing communication protocols, such as encrypted tunneling through a VPN

Additionally, financial institutions must adhere to specific regulatory requirements, such as the cybersecurity regulations established by the New York Department of Financial Services and the Interagency Guidelines Establishing Information Security Standards under the Gramm Leach Bliley Act. These mandate ongoing assessment and monitoring of information security programs to ensure that foreseeable risks are identified, managed, and mitigated to the extent feasible, commensurate with the institution's size and complexity.

To date, a majority of companies have adopted some or nearly all of the recommendations advanced by the federal government, many of which involve the acquisition of new applications, software licenses, and cloud platforms, as well as the expansion of existing capabilities.

Transformation and digitalization continue at a rapid pace, and implementation of virtualization (or the process by which physical servers or other machines are distributed among many users and environments) has been accelerated further in many instances as a response to the ongoing pandemic. Several challenges have resulted, including:

- an uptick in personal devices being used for company business
- unapproved software and storage solutions being used to store company information
- inadequate monitoring, data loss prevention policies, and cloud security solutions for cloud services
- inadequate security awareness training

Many of these emerging risks and challenges represent the top concerns that IT and security professionals have today. These concerns are shared by in-house counsel charged with preventing unnecessary liability and reputation damage from data breaches and other cybersecurity events.

Managing New Risks

Unknown or emerging risks that are not captured routinely and managed through a formal risk assessment and review process represent some of the greatest dangers to a business. As a business transforms, risk assessments must transform as well. The introduction of unapproved software and unregistered devices on a company network can degrade even the most robust cybersecurity defenses if not effectively managed.

Personal devices used to store company information may pose threats if they do not have adequate protection from viruses, trojans, ransomware, and other unwanted software. Unapproved storage solutions, such as third-party shared drives or personal email, may create unacceptable risks to data loss and theft, particularly if the information is high value, such as trade secrets, or contains sensitive personally identifiable information (S-PII).

Without a firm understanding of the pitfalls associated with remote work operations, management will struggle to mitigate emerging information security risks. Companies must continue to update risk assessments and develop information security solutions to keep emerging threats at an acceptable level. The risks include using, maintaining, or expanding third-party vendors for VPN, cloud storage, email, and other business applications.

Classifications, De-identification, and Access

One method for managing information security risks is to reexamine traditional approaches to information classification and access control. Refining policies for classifying information based on its sensitivity and importance, as well as limiting access to sensitive information through the principle of least privilege can allow a company to manage information security risks effectively. This approach reduces access to individuals who need it, and focuses resources toward information that is most in need of protection.

For example, a company with only three levels of classification (sensitive, PII, and public) may consider further sorting information into additional categories. For example, trade secrets and financial information may both be classified as sensitive, but unauthorized disclosure of trade secrets could carry greater harm than unauthorized disclosure of nonpublic company financials. A three-tiered classification system may not capture this distinction.

Concurrently, employees requiring access to trade secrets may differ from those requiring access to company financials. Each group should only have access to the information required. Many cloud providers offer increasing flexibility with respect to role-based access controls, and they may assist companies in implementing such controls based on the principle of least privilege. S-PII confidentiality risks may also be managed by de-identification procedures, such as replacing direct identifiers (e.g., name and social security number) with artificial identifiers. This also has the effect of enhancing overall privacy protections and reducing potential reputational, financial, and privacy impacts of unauthorized disclosure.

By reducing the number of users with access to particularly sensitive information and further classifying information, a company can reduce its overall threat landscape.

Bring Your Own Device

Companies should determine if their policies adequately cover Bring Your Own Device (BYOD), personal cloud storage, home-office security, and incident reporting. Even if such topics are covered in the company's existing information security program, the increased volume of non-company issued devices, third-party storage solutions, endpoints, and the sensitivity of the information authorized to be processed on those devices may affect the overall risk assessment and require additional controls.

A formal remote access policy that is sufficiently detailed in these respects assists a company in setting standards and expectations for BYODs and facilitates communication to the workforce. Without formal policies, employees will often take matters into their own hands by transmitting confidential company information via unapproved third-party applications.

BYOD also provides a host of legal issues that must be considered, including data ownership, employee privacy, monitoring, data loss prevention, encryption, and data retention, particularly in the context of litigation holds. Personal devices require additional management and acknowledgement by the employee of certain rights by the company to access and monitor the device. A traditional remote access policy may not sufficiently cover these issues, and, therefore, the company should adopt a more comprehensive policy.

Cloud-Based and Other Third-Party Applications

More companies are leveraging cloud solutions and cloud applications to support remote work, but research, such as the 2020 Verizon Data Breach Investigations Report, suggest that those companies' cloud-specific security and data loss prevention solutions are inadequate. The issue of sensitive data protection is a challenging one, as many companies continue to struggle between the accessibility of sensitive information, such as trade secrets, and the continuity of its operations.

Cloud technology provides a convenient, scalable, and flexible way to enable telework, but cloud-specific monitoring, data loss prevention, and access control must be implemented to prevent external and insider threats (both malicious or inadvertent). NIST guidelines note that cloud security generally requires cloud-specific solutions that may not be consistent with the solutions implemented for traditional network boundaries.

In April 2020, the Federal Financial Institutions Examination Council highlighted these specific issues and issued updated interagency guidelines that, among other things, require financial institutions to manage the specific risks associated with cloud service providers. For example, cloud service-provided security solutions, commonly known as cloud access security brokers, may not completely cover the requirements of a financial institution's information security program, and may require complementary third-party security solutions.

Reviewing Cyber Insurance Policies

Companies should review and evaluate the sufficiency of their cyber insurance policies to ensure that telework-associated risks are adequately covered. A change in the risk profile of a company (as a result of telework) may prompt a company to consider whether its information security policies adequately cover:

- first-party (company costs) and third-party (liability to consumers) costs associated with an incident
- costs associated with incident response, including notification, forensic investigations, lost or stolen devices, and legal fees
- loss associated with insider threats (both non-malicious and malicious)
- costs associated with recovering from ransomware or other disruptive events
- social engineering or phishing attacks

Furthermore, cyber insurers, in response to the increasing adoption of remote work, are seeking more information regarding a company's approach to incident response, business continuity, and other cybersecurity events. They may also want to review supporting plans. Consequently, ensuring that adequate incident response plans, continuity plans, and other risk mitigation plans are documented may assist companies in obtaining good cyber insurance.

Conclusion

The cyber threat landscape is still evolving with respect to telework operations, but many emerging risks should be addressed sooner rather than later, particularly if a company is considering long-term teleworking.