ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

5 Cybersecurity Tips for the “Flipped-turned Upside Down” World

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***Be proactive.*** Review or implement risk prevention and monitoring standards, like multifactor authentication, data loss prevention, reduced use of personal devices, cloud technology, and backup procedures.
- ***Keep up to date.*** Update your cybersecurity and remote work policies and institute regular training for employees.
- ***Know your insurance.*** Review your cyber insurance coverages and limitations.
- ***Find the right personnel.*** Choose credentialed, senior-level executives to lead multi-dimensional cybersecurity practices.

To quote Will Smith and DJ Jazzy Jeff from their intro song to the hit TV show Fresh Prince of Bel-Air:

> *Now, this is a story all about how*
>
> *My life got flipped-turned upside down*
>
> *And I'd like to take a minute*
>
> *Just sit right there*
>
> *I'll tell you how I became the prince of a town called Bel-Air*

While we would love to tell you how to become a prince, we are much more adept at giving you tips on how to help prevent and mitigate a data breach in this "flipped-turned upside down" world!

The COVID-19 pandemic upended daily routines, and as cities instituted stay-at-home orders, many people found themselves suddenly working from home. The pandemic has accelerated the shift to remote workforces, and we have all seen a digital transformation driving business productivity, continuity, and survival. Even as restrictions lift and people return to corporate offices, much of tomorrow's workforce will move seamlessly between corporate and home office environments as employers adopt flexible working arrangements and technology continues to drive new ways of doing business. Organizations must pay close attention to operational security gaps in new work environments and reevaluate security processes and procedures. Because employers have fewer controls and physical safeguards over home networks and personal devices, remote work environments create increased opportunities for accidental or criminal security breaches. The digital response to COVID-19 exposed these gaps, as attackers are increasingly targeting remote vulnerabilities to gain access to valuable proprietary business information.

Overcoming the security gaps of a remote workforce requires embracing best practices, rethinking existing security protocols, investing in emerging and innovative technologies, and updating policies

and procedures to address and control against these dynamic threats. By taking a proactive approach, organizations can limit the financial and reputational risks associated with data breach incidents and protect the interests of clients and customers.

As more employees work from home, organizations need to work closely with their security officers and IT professionals to review their cybersecurity practices and understand what is working, respond to potential new threats, and close any vulnerabilities to ensure remote work environments protect valuable business information, including personal and financial data, protected health information, and other sensitive and proprietary information. This is especially important for smaller and mid-size companies, which are often seen as easier targets for cybersecurity breaches. Now is the perfect time to review your remote work systems, tools, and policies, and assess and correct gaps in remote work environments to ensure information accessed anywhere remains secure.

With that in mind, here are five steps to incorporate into your organization's cybersecurity framework:

1. Review or implement risk prevention and monitoring standards.

Multi-factor authentication (MFA)

Implementing MFA is one of the simplest and most effective tools an organization can use to help prevent unauthorized access.

MFA is a method of computer access control that requires users to provide authentication methods from at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).

For remote working, MFA should always be enabled when accessing networks or systems outside the office. MFA should be required for all remote access as well as for any webmail. This ensures that if an employee's password is ever compromised, an attacker will not be able to access sensitive information without the employee's mobile phone.

Data loss prevention (DLP)

With remote workers accessing and transmitting data from home, implementing DLP can help an organization stop data from inadvertently being sent to third parties without proper authorization or protection. DLP technology scans data leaving the organization in documents, emails, and other forms for Social Security numbers, personally identifiable information, personal health information, or other sensitive or critical data, and blocks the transmission if these types of data are found. DLP can also include scanning data going onto removable media for physical transport.

Reduce usage of personal devices

Organizations can reduce and manage risk by controlling the equipment that employees use when working from home. Employer-issued laptops, WPA3-enabled routers, and other devices with minimum standards of encryption and antivirus protection can help ensure safe work practices. Employees, particularly those with access to sensitive and confidential documents, should be prohibited from downloading files to their personal devices outside of the network or working offline, which can compromise data files and leave files open to loss or disclosure to third parties.

By issuing company-owned equipment, organizations can in turn control all settings associated with security and access to data and transmission of that data.

Evaluate cloud-based systems and other digital applications

With large portions of the workforce working remotely, organizations have embraced applications that permit employees to access their information and systems on the cloud, attend virtual meetings, and collaborate and chat online. In many cases, technology can help a company become more resilient to cyberattacks. Utilizing cloud technology can ensure that systems and important data are accessible anywhere in the world.

> **Because employers have fewer controls and physical safeguards over home networks and personal devices, remote work environments create increased opportunities for accidental or criminal security breaches.**

While new technology has revolutionized remote work productivity, new software applications and service providers should be thoroughly vetted by IT and security teams to avoid introducing inadvertent security risks. With more employees working remotely, organizations should also review existing contracts with cloud service providers, IT service providers, and other third-party vendors and suppliers to ensure such contracts include appropriate security protocols and obligations for any data exchanged by the parties.

Implement backup procedures

Backup procedures and the restoration processes should be tested quarterly. They should be reviewed, maintained, and revised on a periodic basis.

Having proper backup procedures of all essential systems and services will not only lead to quicker recovery when having to restore, but also ensure that there is no data loss in the event of a cyber incident. For example, it is essential to protect against interruption from a ransomware attack by regularly performing backups of files and systems. Such backups should be stored separately so they cannot be accessed on the main network.

2. Update your cybersecurity policies and remote work policies.

Cybersecurity and information security policies

Policies should be documented, accessible, and understood by all employees.

Cybersecurity and information security policies should be specific to a company and will vary depending on industry, size, network infrastructure, and information collected. Such policies should inform employees regarding network assets; identify the primary threats to those assets; describe acceptable use (including protocols related to password management, secure file transfers, software updates, malware scans, use of social media and privacy settings, and other security guidelines designed to protect against cyberattacks); and provide a roadmap in the event of a security incident.

Such policies should be reviewed regularly to ensure compliance with federal, state, and industry-specific breach requirements, as well as consumer privacy laws such as California’s Consumer

Privacy Act (CCPA) or the European Union's General Data Protection Regulation (GDPR), to the extent applicable.

Breach response is an extremely important component of cybersecurity and information security policies. There should be an established data breach incident response plan for responding to and recovering from potential incidents that outlines responsibilities, actionable steps to be taken, and notification plans. This plan should be tested at least annually.

> **While new technology has revolutionized remote work productivity, new software applications and service providers should be thoroughly vetted by IT and security teams to avoid introducing inadvertent security risks.**

Review business continuity policies and procedures to ensure the continued protection and availability of sensitive data during adverse or disruptive situations. Test business continuity plans at least annually and update those plans whenever security incidents, significant changes to business operations, or changes to the regulatory environment require or justify an update.

Remote work policies

Many workplace and security policies only minimally address remote work. To that end, it may be appropriate to create new policies or update and review existing policies to address remote work standards.

A remote work policy should provide clear guidance to employees on how to connect to the system (via VPN and/or with certain complex password protocols or multi-factor authentication), rules for internet usage while accessing the system, what devices are acceptable (personal or employer-issued devices) and restrictions on friend and family use of such devices, and any technology that may be used to monitor remote work. Home wifi networks should be password protected, and devices used for work purposes should be passcode enabled.

> **Despite meeting the highest operational and technology standards, there will always be a human element and no network can be 100 percent secure.**

Clear communication of remote work policies will help ensure consistent employee practices and expectations. In addition, employees, particularly those who are less tech-savvy, should be encouraged to seek support from their IT team as they transition between office and remote work.

3. Continue education and regular cybersecurity training for remote employees.

Despite the growing sophistication of cyberattacks, many still rely on human error (clicking an email link or opening an attachment) for their success. Administrative and technical safeguards will not fully protect employers if they do not also regularly train and educate their employees to recognize cyberthreats. Organizations must be vigilant in their efforts to train employees on what is required of them for security and compliance purposes and prepare them for email phishing attacks or other security threats. In addition to formal training, successful security awareness programs send frequent reminders to employees on common or recent security threats and test preparedness on an ongoing

basis, through quizzes or simulated email phishing campaigns.

Cybersecurity training programs establish safe and secure methods to carry out employees' daily responsibilities and heighten awareness of common practices bad actors use to gain unlawful access to systems. Training programs should be mandatory for all employees and conducted regularly.

Employers must encourage and maintain communications with their remote employees. Particularly where the transition to remote work was abrupt, leadership should check in regularly to gauge their employees' ability to work effectively from home, identify any technology issues or support needs, and provide opportunities for employee groups to engage and collaborate virtually. Employees should feel comfortable communicating with IT and security teams about any suspicious activity or security threats. Just as in the office, remote employees should be aware of what they must do if they receive a security alert and the urgency of reporting any security threats or incidents to appropriate management.

4. Review your cyber insurance coverages and limitations.

Maintaining a secure environment, particularly one that involves a remote workforce, is a process. Despite meeting the highest operational and technology standards, there will always be a human element and no network can be 100 percent secure. Due to the high level of cyber risk in today's business environment and exclusions for cyber events in other types of insurance policies, a cyber liability insurance policy is a must.

> **People and processes are the foundation of mature cybersecurity programs. Companies must have policies that focus on best practices and governance and subsequently train all employees on these policies or the technology will be of little use in protecting the company.**

A proper cyber insurance policy should include reimbursement for investigation, business loss, required notification and credit monitoring to clients, legal expenses, cost of extortion, and cover human error where possible. Terms and exclusions contained within cyber insurance policies vary widely, and companies should select and review cyber policies carefully to ensure the policy adequately addresses unique risks or vulnerabilities.

Policy exclusions, such as coverage exclusions for failing to obtain minimum security standards, can be a trap for the unwary. Companies should review their policies and ensure they adopt necessary cybersecurity measures with respect to remote work environments, so they do not undermine their coverage. Policy limits should also be reviewed to ensure that limits meet expectations of guarantees that have been agreed to in contracts with third parties.

5. Put the right personnel in charge to lead multi-dimensional cybersecurity practices to battle increasingly complex cyber-risks.

Companies should have a credentialed, senior-level executive with the designated responsibility of establishing and maintaining the enterprise vision and strategy of a comprehensive cybersecurity program for the entire organization to ensure information assets, systems, and technologies are adequately protected.

People and processes are the foundation of mature cybersecurity programs. Companies must have policies that focus on best practices and governance and subsequently train all employees on these policies or the technology will be of little use in protecting the company. Setting the right tone for cybersecurity from the top is critical. It's recommended that companies take a step further and hire information security professionals or a reputable third-party security officer with the right knowledge and skills to implement cybersecurity practices and protocols that cover risk assessment, threat prevention, and incident response.

Key takeaways

A data breach can have devastating consequences, including financial loss, business interruption or shut down, and long-term reputational harm. The COVID-19 crisis has fundamentally changed the way we work, and time will tell if widespread telecommuting becomes more permanent. By implementing controls to access network systems, taking steps to identify and protect sensitive and proprietary information, and educating and supporting employees in remote work environments, organizations will strengthen trust among their employees, customers, and business partners, and be more resilient during this crisis and into the future. Life may be "flipped-turned upside down," but following these tips can help ensure your organization is protected and prepared to navigate cybersecurity risks in this new remote-work world.

ACC EXTRAS ON… Cybersecurity

ACC Docket

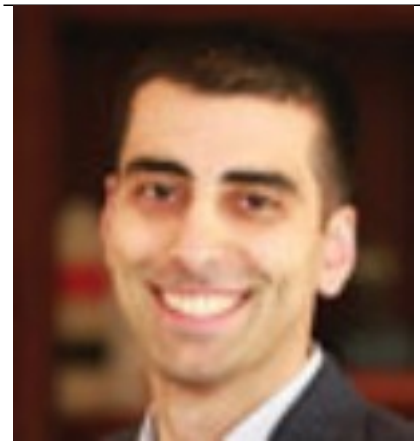
Cybersecurity in the Age of COVID: How to Protect Your Data (Aug. 2020).

5 Cybersecurity Tips Your Mother Taught You (Jan. 2020).

Cybersecurity: The Achilles Heel of Today's Global Law Departments (Nov. 2019).

ACC HAS MORE MATERIAL ON THIS SUBJECT ON OUR WEBSITE. VISIT WWW.ACC.COM, WHERE YOU CAN BROWSE OUR RESOURCES BY PRACTICE AREA OR SEARCH BY KEYWORD.

Gulam Zade



CEO and General Counsel

LOGICFORCE

Gulam Zade is the CEO and general counsel of LOGICFORCE, an IT consultancy. He is chair of ACC's Small Law Department Network and serves as treasurer for ACC Tennessee.

Willa Kalaidjian

Cybersecurity and Data Privacy Group Chair

Chambliss

Willa Kalaidjian is the cybersecurity and data privacy group chair at Chambliss, a member of Meritas, the premier global alliance of independent law firms. She is based in Chattanooga, TN. She

is based in Chattanooga, Tennessee.