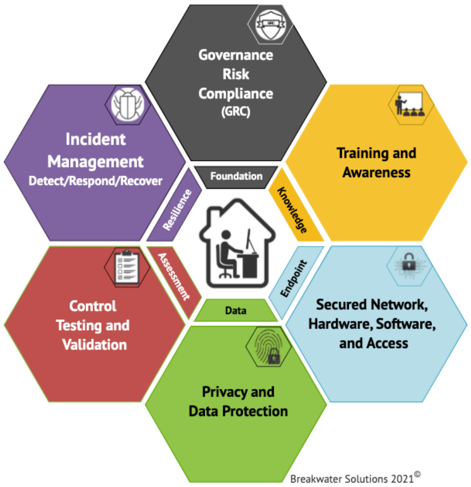
Remote Workforce Security

Recent studies from Pew Research (KIM PARKER, 2020) and OWL Labs (Labs, 2020) reported over 70% of full-time workers in the U.S. are now working remotely as a result of COVID-19; a stark contrast from the 6% who recently reported themselves as remote workers to the US Census Bureau (Bureau, 2021). These trends are being seen globally, with experts citing that 51% of all knowledge workers worldwide will be working remotely by the end of 2021 (Gartner Newsroom, 2021).

This previously unwelcome shift to a predominantly remote workplace has helped companies remain competitive in today's challenging economy and has yielded several unexpected benefits, including a significant widening of corporate access to a more global employee and consumer marketplace. Realization of those benefits; however, must be met with a healthy respect for the risks that come with them; cybersecurity being one.

Generally regarded as the first line of defense, individuals are often the primary targets of cyber-attacks. This threat is compounded significantly when those individuals work remote in uncontrolled environments and often on uncontrolled devices. Knowing and addressing your cyber risks as they relate to a remote workplace is critical, but the rewards of doing so are significant, and can help a company realize significant monetary gains and employee goodwill.



Breakwater Solutions 2021©

Breakwater Remote Workforce Cybersecurity Framework

Protecting your most precious assets requires a multi-pronged remote workforce security strategy. Our framework addresses remote workforce cybersecurity holistically and includes:

- Governance, Risk, and Compliance
- Enterprise Training and Awareness
- Secured Endpoints and Productivity Tools
- Strong Authentication and Authorization
- Data Privacy and Protection
- Control Testing and Validation
- Incident Management
- Cyber Resilience

Remote Workforce Cyber Program Assessment

Using Breakwater's Remote Workforce Cyber Security Framework as our guidepost, our team will perform a comprehensive review your remote workforce program to help you identify your most pressing cybersecurity gaps. We'll work with your 2nd line risk and compliance teams to validate that policies, governance, and oversight have been comprehensively documented and adopted, and we'll work with your 1st line IT and Cyber teams to validate those technical controls have been adopted, and their efficacy regularly vetted, to provide you the greatest degree of assurance that your enterprise crown jewels are resilient from cyber-attack.

Where independent control effectiveness testing is requested, Breakwater's technical assessment services can be engaged and incorporated into our overall program analysis to provide a greater degree of assurance that implemented controls are not only comprehensively designed, but also effectively operating.

Governance, Risk and Compliance Program Review

A successful remote workforce cybersecurity strategy begins foundationally with enterprise policies and standards that define an appropriate set of controls that must be implemented to provide layered defenses against cyber incidents. Once implemented, corresponding controls are then independently governed and tested for compliance to provide a layered set of defenses against potentially material program gaps.

Breakwater's Remote Workforce GRC review is designed to identify control gaps in an enterprise's policies and standards, and then further assesses gaps in how those policies and standards are independently governed and reported on to senior management.

Where additional help is needed to fill programmatic gaps, Breakwater's tenured executive cyber team members can work with varied stakeholders to develop policies, standards, guidelines, and procedures that will help ensure a solid foundation upon which to securely manage your remote workforce.

Training and Awareness Program Review

A key component to a successful remote workforce strategy is the ongoing awareness and education of your remote workers. As end-users are regularly the first target of, and the first line of defense against, hostile cyber criminals, it is imperative that they learn and keep up to date on the skills they need to be part of the enterprise solution to battle cybercrime. They should know how to respond to cyber-attacks, and their knowledge and diligence should be tested regularly. Breakwater will review your current training and awareness program and help identify opportunities for improvement to better inform and engage your remote workers to make them a key part of your cyber solution.

Endpoint Control Program Review

Establishing a secure technical environment and enabling a remote workforce with the right tools to securely perform their jobs is paramount to a successful remote workforce cyber strategy.

Breakwater's Endpoint Controls Program Review will examine an enterprise's network and remote access solutions, productivity and telecommunications tools and technologies, and identity and access management solutions. Our key objectives are to help ensure that an enterprise's remote workforce solutions meet the spirit of applicable internal and external security and compliance requirements, and that they meet the operational needs of end-users. A breakdown in either of those areas often results in security gaps and "workarounds" that ultimately result in loss.

Privacy and Data Protection Program Review

A successful remote workforce strategy incorporates technologies and practices that maintain control over an enterprise's information regardless of where it is accessed or resides. This is particularly important for companies that have embraced a remote workforce strategy that requires access to highly sensitive information from an almost limitless array of non-captive working environments.

Breakwater's Privacy and Data Protection Program Review examines the global privacy and data protection implications of how an enterprise has implemented its remote workforce solutions. We examine the preventative and detective controls in place to prevent improper data disclosures or privacy breaches in one or more global jurisdictions. We go a step further to examine privacy and data protection from the perspective of the remote workers themselves; recognizing that the protections afforded employees by having physical separation between work and home no longer exist in a remote workplace, and often results in heightened risk of cyber-attacks to home networks and personal devices.

Control Validation Program Review

Ensuring for the efficacy of a remote workforce cyber security strategy requires multiple layers of control validation that includes testing in the 1st line of defense where controls are implemented, and independent validation by members of the 2nd and/or 3rd lines of defense in Corporate Risk and Internal Audit.

Breakwater's Control Validation Program Review will examine the governance structure of an enterprise's remote workforce strategy to ensure that controls are regularly, comprehensively evaluated, and that gaps are addressed in an appropriately timely fashion.

Control Cyber Incident Management Program Review

Implementing the right mix of preventative cyber controls into an environment is often a complex balancing act that pits cost against reward and rarely, if ever eliminates all risk from the equation. It therefore stands to reason that incidents will happen and enterprises must be prepared to identify and address those incidents in a timely fashion.

Breakwater's remote workforce Cyber Incident Management Program Review examines a comprehensive array of incident management aspects, from how incidents are identified across the global remote workforce footprint, to how workforce environments are segmented from non-workforce environments, to how actualized threats are addressed with the least amount of impact to remote workers, to how processes, data, and operations are backed up and restored in an appropriately timely fashion. All functions must operate fluidly and harmoniously for an enterprise to recover in an appropriately timely fashion.

Areas of Expertise

- Virtual CISO (fractional/interim)
- Cyber program development
- Cyber risk management
- Data privacy, governance, and analytics
- Threat and vulnerability management
- Digital Forensics & Incident response
- Regulatory compliance and oversight
- Cyber talent mentoring & development

Our Differentiators

- **Team Approach.** Breakwater's executive cyber risk officers will provide a dedicated point of contact, backed by a team of tenured cyber risk subject matter experts, to preserve program continuity throughout an engagement
- **Seasoned Experts.** Breakwater's team of field-tested cyber risk professionals will bring knowledge, experience, and sophistication to each engagement to ensure program success
- **Tailored Program.** From a one-time project to interim oversight to permanent placement, Breakwater's executive cyber risk officers will customize a program that suits an organization's specific needs

About Breakwater

Breakwater helps mitigate risk and gain insight from sprawling information by combining technology automation and human expertise. Our expert consulting, software, and managed services address the challenges within information governance, disputes and investigations, regulatory compliance, privacy, cybersecurity, and legal operations. Our solutions allow governance, legal, and risk professionals to locate, access, analyze, and manage information by making data transparent and actionable. Breakwater helps clients in public and private sectors mitigate risk, improve productivity, and increase profitability by transforming how they use data.