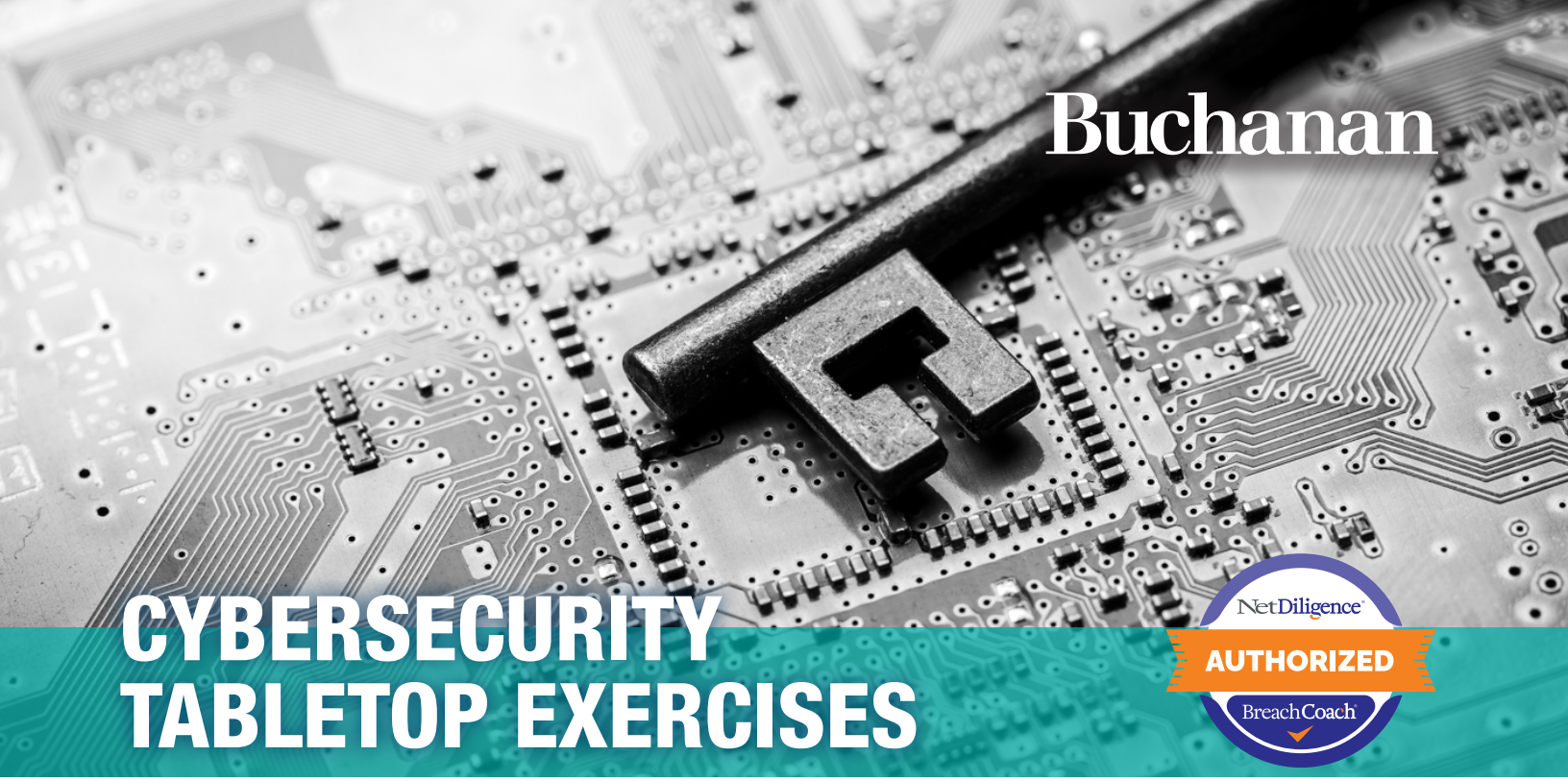

Buchanan

CYBERSECURITY TABLETOP EXERCISES

NetDiligence AUTHORIZED BreachCoach

Real Threats, Real Solutions: Preparing for Cyberattacks with Best-In-Class Capabilities

Cyberattacks are one of the most complex challenges businesses face today. Malicious hackers disrupt operations, immobilize revenue-generating activities and even force businesses to close. Attacks have become more likely and severe as threat actors become highly sophisticated at identifying system vulnerabilities, deploying phishing emails and exploiting the rise of remote work. These events touch nearly all business operations, demanding whole-of-organization responses. Companies must prepare with realistic and tested plans and protocols that involve all departments, not just IT. Buchanan has the expertise to address the technological aspects and business challenges of cyberattacks, coupled with the experience to lead businesses through disruptions and sustain operations until devices and systems are restored to normalcy.

Why Have Tabletop Exercises?

- **Prepare** incident response teams for a variety of risk scenarios
- **Simulate** real-world, dynamic threat situations
- **Encourage** cross-organizational collaboration and discussion
- **Identify** gaps in incident response plans

Today, every business uses information technology to conduct its core activities and store sensitive digital information, including the company's own data and the confidential information of customers, clients, staff, leadership, and partner organizations. Cybersecurity tabletop exercises simulate a multi-faceted cyberattack on your business. They are an essential tool to assess organizational readiness and to sharpen the skills and habits your team will need when responding to complex cyber threats and incidents.

As one of the select few firms in the world recognized as a NetDiligence Authorized Breach Coach® law firm, Buchanan's legal teams have worked with countless organizations to think through technology's most challenging problems and develop cybersecurity policies and procedures tailored to the unique threats each company faces. We work with leadership to strengthen the awareness of every person in the organization, so that they know who to contact if they suspect a cyber incident is developing, how to access their cybersecurity playbook, and what to do in the event of an attack.

Our Unique Approach

The Buchanan team has developed a proven, multi-step framework for our cybersecurity exercises that drives our methodology. Guided by this approach, each engagement includes the following:

Discovery

- Thorough interviews with the organization's security team, general counsel, and business operations leaders to understand processes and the organization's unique needs
- Assessment to evaluate current security measures and business continuity plans in the event of a cyber incident
- Identification of primary decision makers and cybersecurity leaders

Initial Plan Development & Review

- Initial incident response plan development and review with key stakeholders, security teams and leadership

Initial Tabletop Session

- Abbreviated tabletop session to evaluate initial incident response plans against realistic cyber incident scenarios
- Modifications to incident response plans to address gaps identified during initial sessions

Formal Tabletop Exercise

- A four to six hour tabletop exercise, with participants appearing virtually or in person, featuring key stakeholders such as business operations representatives, legal teams, c-suite leaders, and information technology professionals, during which scenarios and response plans are tested to review organizational awareness, identify strengths, weaknesses, and gaps, and diagnose alignment to legal, regulatory, and contractual requirements
- Recurring tabletop exercises every six months, or as frequently as necessary, to update plans and prepare for new scenarios, informed by evolving cyber threat developments and malicious actors' practices

Fire Drills

- Unannounced mini-tabletop sessions, or fire drills, to update and reinforce previous lessons learned, and to instill a culture of rapid response, maximum security, and continued preparedness

Periodic Training

- Other training exercises to plan for emerging issues or boost skills and preparation of specific departments and teams to play their unique roles, as needed

ADVANCING OUR CLIENTS' GOALS

- Delivered tailored tabletop exercises to enhance preparedness and response capabilities for a diverse range of industries. Developed real-world simulated scenarios for hospitals, banks, emergency response services, global manufacturers, and national construction companies, based on geopolitical and industry-specific threats to ensure each client is well-equipped to handle threats to their organization effectively.
- Helped a Fortune 500 company respond to and recover from a complex ransomware attack, developed a framework for non-materiality under SEC rules, and guided the client through an SEC inquiry.
- Led response efforts for financial sector entity hit by a ransomware attack on 100+ banks and credit unions, implementing swift remediation strategies and boosting security measures against future threats.
- Managed a high-stakes investigation into business email compromise and wire fraud at a growing M&A-active company, partnering with U.S. Secret Service to recover misappropriated funds and safeguard financial integrity.

Tabletop Exercises: The Key to Modern Cyber Protection

With Buchanan's cybersecurity tabletop exercises, companies are prepared with best-in-class capabilities, processes and strategies to overcome cyberattacks.

Planning

- Train entire organization on cybersecurity processes and systems for routine operations and incident response
- Formalize suspected and confirmed incident investigation procedures
- Assign cybersecurity and business continuity responsibilities

Prevention

- Identify cybersecurity and incident response planning issues
- Improve network visibility and data management
- Close infiltration points and protect against vulnerabilities including third-party access
- Implement strategies to help reduce the likelihood of an incident occurring

Response

- Mitigate cybersecurity incidents from the moment of discovery
- Use formal cybersecurity playbooks to accelerate incident response actions
- Preserve and manage digital and other evidence

Compliance

- Provide actionable insights on how to stay compliant with cybersecurity and data privacy requirements, including regulatory standards, legal review, data mapping, and notification
- Document the legally compliant security program, which is critical in defending a data breach investigation and litigation

MICHAEL G. MCLAUGHLIN
Co-Leader of Buchanan's Cybersecurity and Data Privacy Group
michael.mclaughlin@bipc.com
202 452 5463 | Washington, DC

SUE C. FRIEDBERG
Co-Leader of Buchanan's Cybersecurity and Data Privacy Group
sue.friedberg@bipc.com
412 562 8436 | Pittsburgh, PA

KURT SANGER
Cybersecurity Counsel
kurt.sanger@bipc.com
212 440 4487 | New York, NY

BIPC.com/cybersecurity-and-data-protection