R. McCONNELL GROUP PLLC

A BOARD GUIDE

Cybersecurity & Breach

A board guide to security safeguards and incident response

Administrative, technical, and physical safeguards that protect information systems—plus defined procedures for detecting, escalating, and resolving security incidents

2026 | R. McConnell Group PLLC

WHY IT MATTERS

Why Cybersecurity Matters

The question is not whether an incident comes, but whether you're ready

Incidents are inevitable

Given the shifting threat landscape, security incidents are an unavoidable risk

Sensitive data at risk

The organization safeguards personal and financial information of employees and customers

CIA triad

Security protects the confidentiality, integrity, and availability of information assets

Board reporting duty

Leadership reports at least annually on the program and material cyber risk

REALITY CHECK Given the continually shifting landscape, security incidents are an unavoidable risk the organization must be ready to manage

SAFEGUARDS

Three Layers of Protection

Controls organized into administrative, physical, and technical safeguards

Roles & responsibilities

Assign clear ownership for security policy and incident management

Screening & training

Vet personnel and require recurring security-awareness training

Access control

Grant system access strictly on a need-to-know basis

Encryption

Protect sensitive data in transit and at rest

Monitoring & logging

Configure devices to log events and detect anomalies

Vendor management

Assess third parties before they touch sensitive systems or data

Physical & facility security

Restrict physical access to facilities and systems; secure or wipe retired devices and media

INCIDENT RESPONSE

A Systematic Response

A consistent process minimizes disruption and preserves evidence

Report	Route suspected incidents immediately through a single intake channel
Classify	Flag qualifying events as security incidents and notify security officers
Prioritize	Assign urgency and impact scores that drive resolution timeframes
Contain	Isolate or disconnect affected systems to limit spread
Eradicate & recover	Remove the threat and restore systems to a clean state
Learn	Perform root-cause analysis and document lessons learned

THE LIFECYCLE

How an Incident Reaches Closure

Each reported event follows a defined path

- **Detection**
- **Reporting**
- **Classification**
- **Prioritization**
- **Containment**
- **Eradication**
- **Recovery**
- **Notification**
- **Post-incident review**

ESCALATE

Major incidents trigger notification to senior management—and to legal and authorities where required

KEY TERMS

Definitions

Security incident

An event that may cause unauthorized access, data loss, or service disruption

Internal threat

A user misusing resources, running malicious code, or seeking unauthorized access

External threat

An outside actor attempting to access systems or disrupt service

Chain of custody

Documented, unaltered handling of evidence to support legal action

FOR THE BOARD

Questions the Board Should Ask

A few questions test true cyber preparedness

1

How quickly are critical incidents detected and escalated?

Response timeframes should match the severity of the threat

2

Do we test our incident-response plan regularly?

Preparedness must be validated, not merely documented

3

Are third parties with system access assessed?

Vendors are a common and material avenue of compromise

4

What is our process for notifying authorities and individuals?

Readiness to meet breach-notification duties is essential

Firm Lawyers

Matthew Boyden

is a trial lawyer and former federal prosecutor with more than thirty-five years of experience. He represents companies and executives in high-stakes criminal, civil, regulatory, and governance matters, and is regularly engaged where litigation risk, regulatory scrutiny, and institutional exposure intersect. His practice includes federal criminal defense, complex civil litigation, internal investigations, and board-level advisory work, including securities, sanctions and trade controls, anti-corruption, and anti-money laundering.

Larry Finder

is a trial lawyer and former United States Attorney with more than four decades of experience handling complex criminal, civil, and regulatory matters of national significance. He represents individuals, corporations, and boards confronting serious legal, institutional, and reputational risk. He served in increasingly senior roles at the U.S. Department of Justice, including Chief of the Criminal Division and First Assistant U.S. Attorney, before being appointed United States Attorney for the Southern District of Texas in 1993.

Ryan McConnell

is a former federal prosecutor and trial lawyer who represents companies, boards, and executives in high-stakes criminal, civil, and governance matters. He has tried nearly twenty federal jury trials and conducted hundreds of investigations involving complex fraud, cross-border enforcement, and sensitive regulatory issues. His practice focuses on federal criminal defense, complex civil litigation, internal investigations, and advising boards and senior executives on matters requiring judgment under pressure.