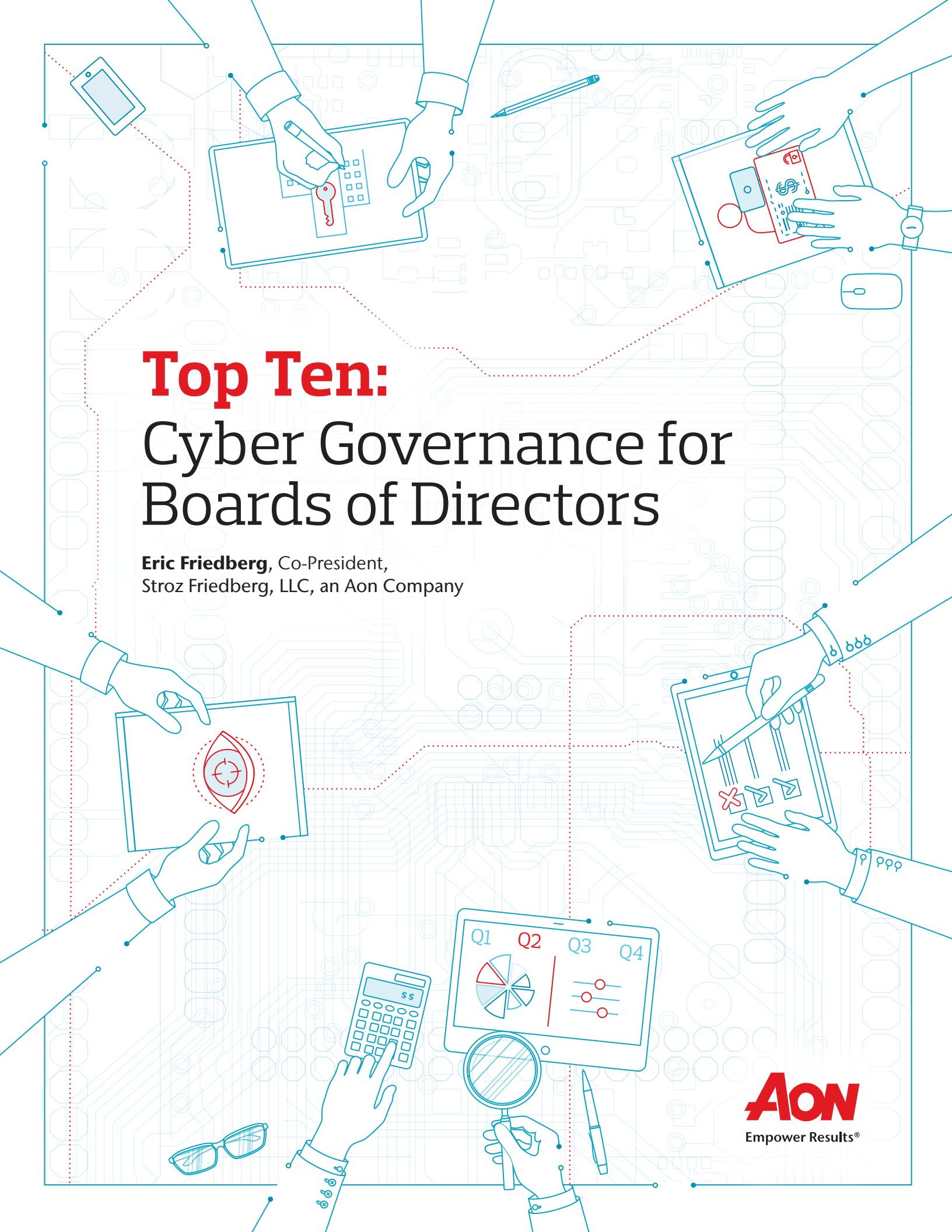
Top Ten:
Cyber Governance for Boards of Directors

Eric Friedberg, Co-President,
Stroz Friedberg, LLC, an Aon Company



AON
Empower Results®

Cyber Governance
Top Ten

Driving great cyber security starts at the very top of an organization. Without the Board and Executive Management setting the tone at the top and driving change regarding cyber, even the most senior cyber security executive cannot alone implement the enterprise-wide changes that result in **materially-enhanced security**.

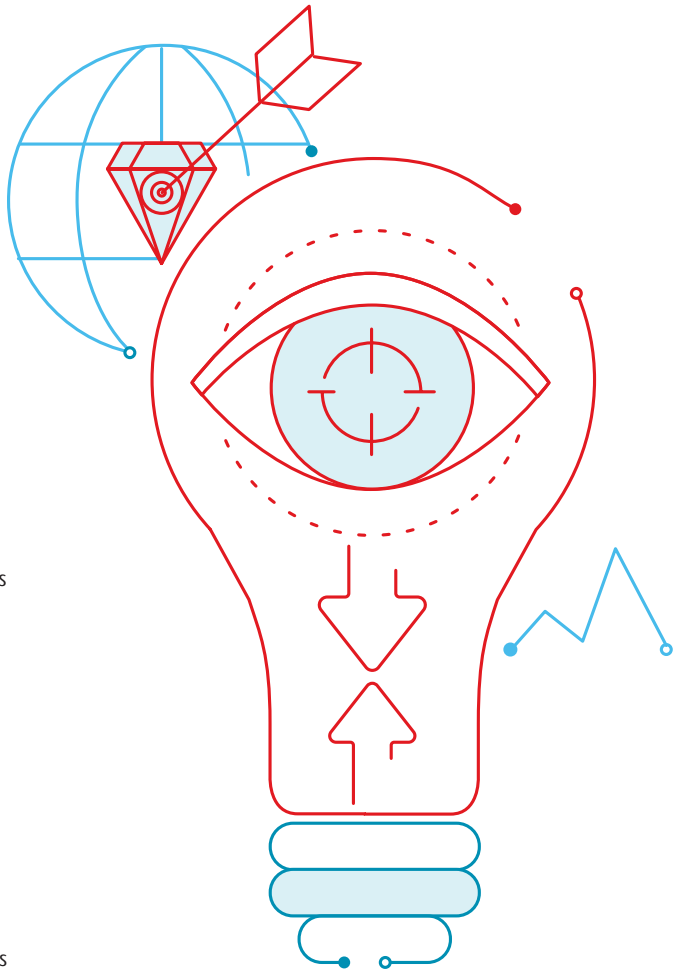
Accordingly, this **Top Ten List** focuses on how a Board can improve its cyber governance. While the Board must also pay close attention to tactical cyber security plans, great governance typically drives great cyber security.

1. **Know What You're Trying to Protect and From Whom.**
2. **Adopt a Recognized Standard for Management and Board Oversight of Cyber Security.**
3. **Set a Target State of Cyber Security.**
4. **Create a Written, Budgeted Security Roadmap.**
5. **Use a Custom Board Dashboard to Oversee Cyber Risk.**
6. **Ensure the Independence of the CISO With Dotted-Line Reporting to the Board.**
7. **Establish a Cross-Functional Cyber Committee.**
8. **Conduct Penetration Testing to Simulate Advanced Attacker Activity.**
9. **Police Third-Party Vendors With Access to Your Network.**
10. **Protect the Balance Sheet Against Cyber Risk.**

1

Cyber Governance: Know What You're Trying to Protect and From Whom.

The cyber security team, Executive Management and the Board need to be aligned about what are the company's **"crown jewels."** Are they proprietary IP, customer data, uptime of an e-commerce site, ability to operate, ability to manufacture or ability to communicate with customers, for example? **A formal threat assessment should:**



- Anticipate how cyber criminals would steal, delete, encrypt or alter valuable data or interfere with key business functions;
- Take into account sector-specific threats as well as the company's unique history of cyber-attacks, if any; and
- Rank the relative likelihood of cyber threats emanating from **state-sponsored actors, financially-motivated attackers, hacktivists and malicious insiders**.

Developing a formal threat assessment will drive discussion about how to prioritize implementation of defenses applicable to each threat group. Since the global threat landscape changes rapidly, the assessment should be **updated every year or two**.

2

Cyber Governance: Adopt a Recognized Standard for Management and Board Oversight of Cyber Security.

While there are various industry-specific or regulator-issued cyber security standards such as HIPAA and HITRUST for health providers and PCI DSS for the payment card industry, such standards often set minimum thresholds that cannot be effectively used to manage overall cyber governance.

One widely-adopted standard for overall management of a cyber program is the **Cyber Security Framework ("CSF") promulgated by the National Institute of Standards and Technology ("NIST")**.

The CSF provides a rigorous framework for objectively assessing the strength of the technologies, policies and staff the company uses in five cyber security areas, which NIST calls "Functions." Those five Functions are Identify, Protect, Detect, Respond and Recover. "Identify" encompasses governance, risk assessment and IT asset inventory. The names of the other Functions are self-explanatory.

The CSF provides an intuitive 1 to 4 grading system for these Functions, which focuses Board oversight. At the lower end the grading range, cyber security policies, technologies or skill sets are patchy, ad-hoc, not risk-based and not enforced. At the high end of the range, cyber security policies are uniform across the enterprise, risk-based, enforced, repeatable, adaptive to changes in the cyber threat landscape and cutting-edge. Grading occurs in 23 very specific categories (which, in turn, contain 108 subcategories) of the Functions.

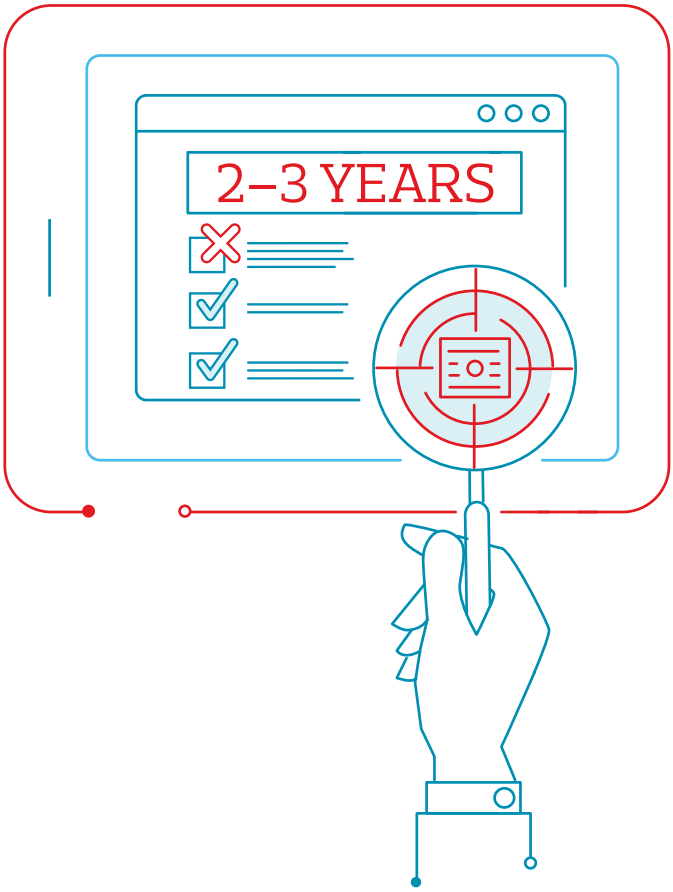
Low grades in one or more specific categories or subcategories can focus the Board and Executive Management's attention on specific technologies, policies, skill sets that are lacking, either completely, or in certain areas of the business. Such objective grading also allows the Board to clearly track progress over time. The Board should insist that Executive Management assess the company's cyber program using the CSF or a comparable overarching standard every two to three years. Assessment work under HIPAA, HITRUST, PCI DSS or other similar industry standards can be mapped to, or relied on in part, for the CSF assessment.

One recommended best practice is to have a **third party expert** conduct CSF assessments until the Board has confidence that Executive Management can self-assess under that framework.

3

Cyber Governance:
Set a Target State of Cyber Security.

As Lewis Carroll said, "If you don't know where you are going, any road will take you there." Once a CSF assessment has measured a company's current state of cyber security (**"Current State"**), Executive Management with the concurrence of the Board should set a target state under the CSF or other overarching standard (**"Target State"**).



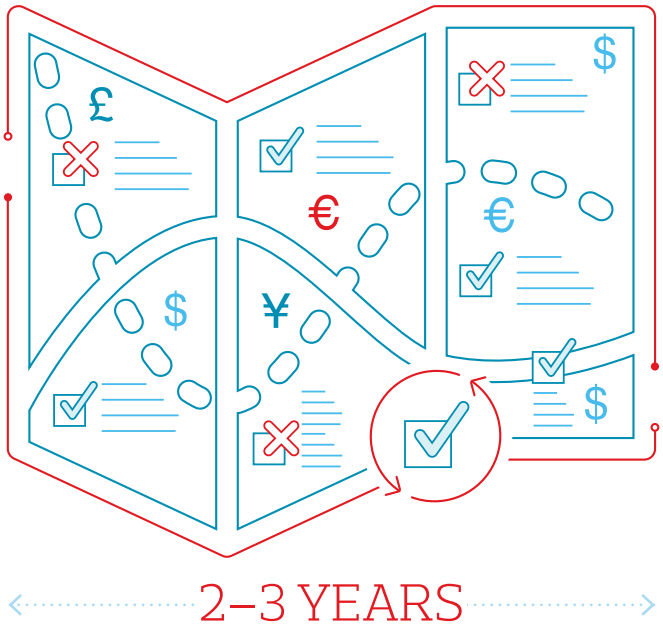
The Target State represents where the company wants its cyber security program to be in two to three years, taking into account its current state, the threat assesment, peer benchmarking, budget and how foward-leaning the company wants to be in cyber. Companies typically aspire to achieve their Target States in two to three years since material remediation and progress under these stringent standards requires a significant investment of time and money.

4

Cyber Governance:

Create a Written, Budgeted Security Roadmap.

Once the Current State has been assessed and the **Target State** is established, Executive Management should tender for the Board's approval a **detailed, written security roadmap**, including management-approved budget to reach the Target State in each Function in **two to three years**. Not surprisingly, in the absence of a written, shared and budgeted security plan and timeline, accountability diminishes, deadlines loosen and progress slows.

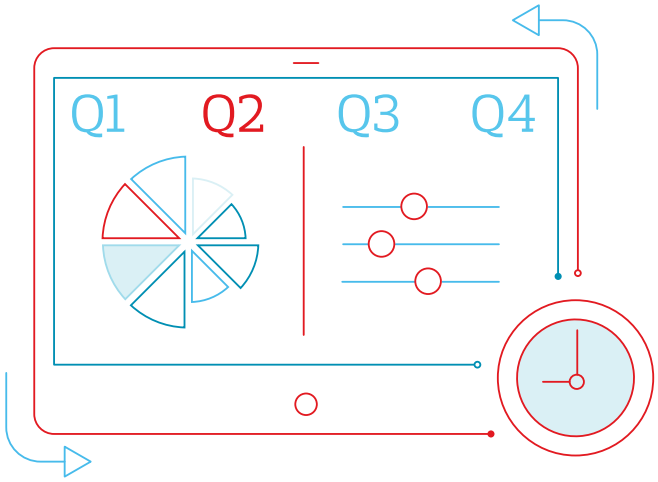


5

Cyber Governance:

Use a Custom Board Dashboard to Oversee Cyber Risk.

Executive Management should present updates to the Board using a **standardized, metrics-driven dashboard** through which the Board can easily view progress (or the lack thereof) against existing cyber security plans.



The dashboard should also include qualitative content that reflects changes in the threat landscape and significant attacks against the company or sector peers. It might show:

- **Annual actual and anticipated progress under the CSF or other overarching cyber standard;**
- **Quarterly progress under the company's written security roadmap;**
- **Quarterly progress with respect to security headcount targets;**
- **Quarterly qualitative descriptions of medium and high severity sector-specific and company-specific cyber security incidents; and**
- **Other data that the Board can use to objectively assess the progress, or lack thereof, in improving the cyber security program.**

The dashboard should not feature relatively meaningless statistics such as how many millions of pieces of commodity malware were blocked by firewalls and intrusion prevention software.

6

Cyber Governance: Ensure the Independence of the CISO With Dotted–Line Reporting to the Board.

Medium–sized companies should have a Chief Information Security Officer (''CISO'') who can independently advise the Board on cyber risk.

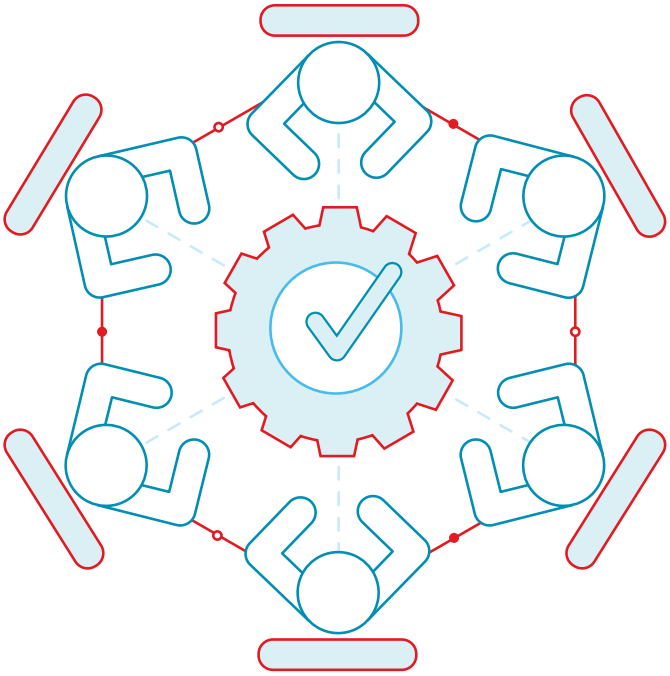
One way to accomplish the CISO's independence is through dotted-line reporting to the Board Audit Committee, including the ability to speak to the Committee in executive session at meetings and directly during a crisis. *Theoretically*, a CISO should not solid-line report to the Chief Information Officer ("CIO"). When the CISO's view of cyber risk is filtered through the CIO, conflicts can arise between dollars spent on infrastructure versus security. In reality, however, many organizations do not have an executive other than the CIO with sufficient technical experience to manage cyber security issues. Giving the CISO some form of reporting line and/or direct access to the Board solves these problems.

7

Cyber Governance: Establish a Cross–Functional Cyber Committee.

The primary sources of cyber threats are organized crime groups, military units of foreign governments, hacktivists and corporate insiders. Incident response often involves a blend of technology, law, investigations, communications, behavioral science and law enforcement liaison.

As a result, the Board should make sure that Executive Management has assembled a **cross–functional committee** designed to support the CISO in the formulation and execution of cyber security strategy.



The committee can include representatives from legal, IT, privacy, communications, human resources and security departments, as well as heads of principal business units. Changes in cyber security that are fully socialized with this group have a far greater chance of being easily and widely adopted. In addition, such collaboration prepares Executive Management for responding to actual cyber events, as most incidents require cross-disciplinary talent to synthesize and sequence work streams devoted to computer forensics, remediation of the network, data breach notification, regulatory obligations, communications to inside and outside constituents, law enforcement liaison, resulting litigation, investor relations and possible insider involvement.

8

Cyber Governance: Conduct Penetration Testing to Simulate Advanced Attacker Activity.

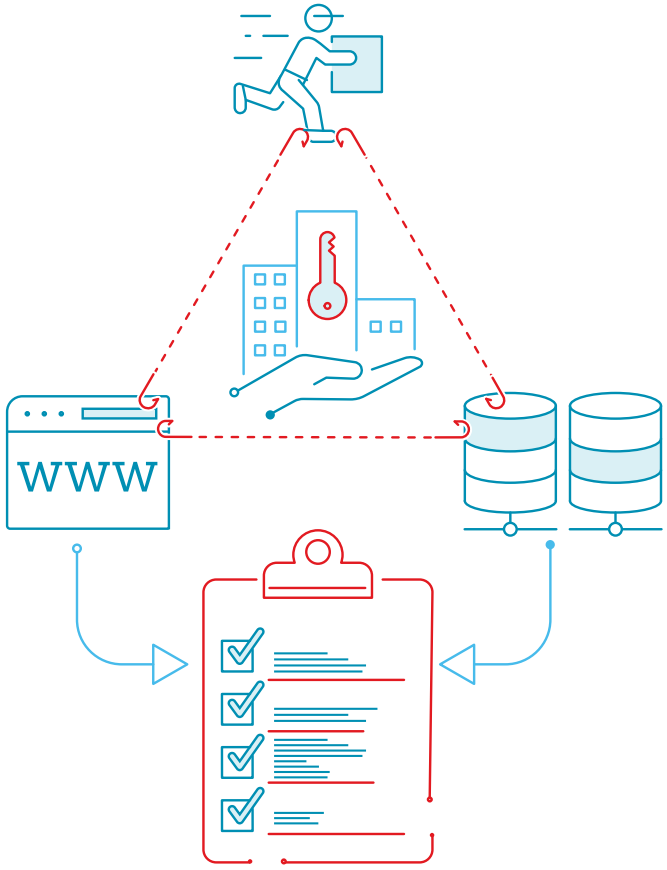
Another recommended best practice is to **employ third parties to find and exploit vulnerabilities before the bad actors do**. The Board can provide oversight in this area by asking a number of questions:

- Do third parties have enough budget, and do they have enough skill, to simulate a sophisticated attack?
- Do identified vulnerabilities get fixed quickly enough?
- How does the company's vulnerability posture and patching schedule compare to its peers' programs?
- Why are the vulnerabilities occurring?
- Are there systematic flaws in the vulnerability management program or the software development life cycle?
- Is the testing schedule comprehensive and fast enough so that all critical servers and applications get tested frequently enough? (Many firms have chosen to double, triple or quadruple their testing pace to complete the entire cycle every two years.)
- When attack and penetration exercises are conducted, does the company's security team detect the attacks early enough to have thwarted them if they were real?

9

Cyber Governance: Police Third–Party Vendors With Access to Your Network.

Hackers often target an insecure vendor to infiltrate a company to which the vendor has remote access, riding the vendor's coattails into the company's network. **The Board should ensure that a stringent program is in place to assess third–party vendors' cyber security.**



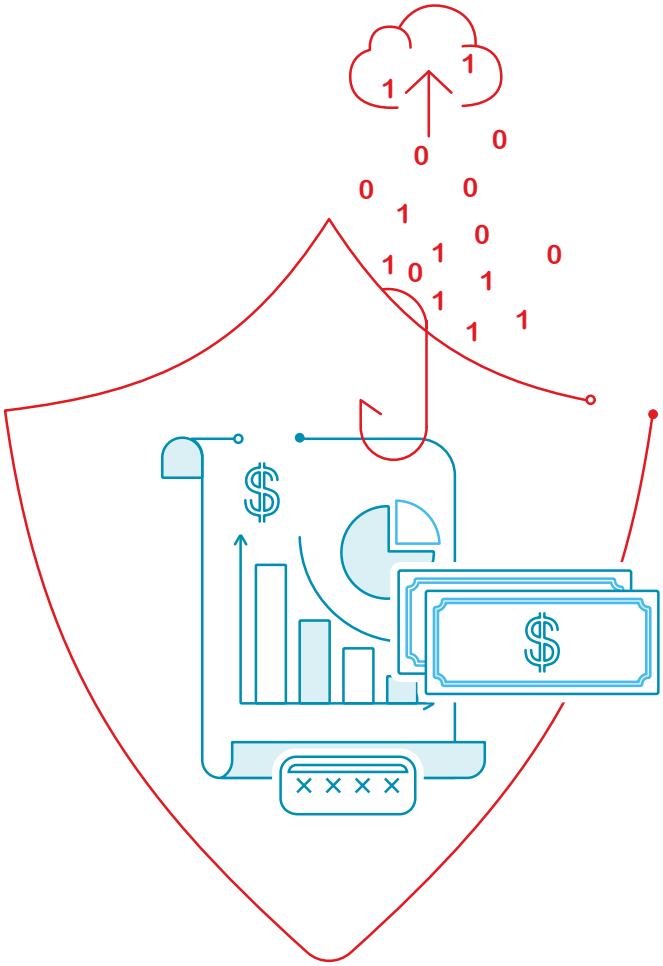
The components of a good program are **a probing questionnaire, strong contractual rights to audit vendors' security programs in the event of a breach or other triggering event, and adequate resources to evaluate vendors' questionnaire responses and conduct necessary audits in a timely fashion**. For companies that have hundreds or thousands of third-party vendors with remote access, cycling through one-third of the questionnaires (and resulting audits) per year for three years takes a small army, and keeping quality control high requires serious budget and sustained focus. Outside gap analyses of the overall program can give a Board better visibility.

10

Cyber Governance: Protect the Balance Sheet Against Cyber Risk.

Coverage provided through cyber insurance can eliminate or lessen significant financial losses in case of a cyber incident.

Covered losses can include the cost of forensic and legal incident response, cyber extortion payments, damaged hardware and business interruption. **The Board should oversee whether Executive Management has calculated the dollar value of the losses anticipated by the threat assessment and whether the company has the right-sized risk transfer policy.**



About the Author

Eric M. Friedberg

Co-President

Education
J.D., Brooklyn Law School
B.A., Brandeis University

Eric M. Friedberg is co-founder and Co-President of Stroz Friedberg, LLC, a cyber consultancy and technical services firm acquired by Aon plc in 2016. Mr. Friedberg has 30 years of public and private sector experience in law, cyber-crime response, cyber-governance, IT security, forensics, investigations and e-discovery. His expertise is sought by boards, audit committees, C-suites, law firms and the courts.

Mr. Friedberg has led responses to some of the most serious cyber-attacks on the nation's companies, including attacks by state-sponsored agents, organized crime, hacktivists and malicious insiders. He is an expert in incident response governance, technologies and policies. He has also conducted enterprise-wide cyber security risk assessments in many business sectors. He has been quoted extensively on cyber-crime and IT security issues in print, digital and television media.

In 2019, Mr. Friedberg was appointed by Governor Andrew Cuomo to the New York State Cyber Advisory Board.

Mr. Friedberg is also a leader in the fields of e-discovery, forensics and privacy, having managed many high-profile assignments in those areas, testified as an expert, been appointed by courts as a Special Master and led the development of new investigative methodologies. He has lectured and published book chapters and articles on e-discovery and forensics. He was previously a member of the Sedona Conference's Working Group 6, the International Association of Privacy Professionals, and the advisory board of The Future of Privacy Forum.

For the 16 years before Stroz Friedberg was acquired by Aon, Mr. Friedberg co-led that firm from a start-up to a 550+ person firm with nine U.S. and four foreign offices. While always a principal business developer and leader of major client assignments, Mr. Friedberg oversaw geographic and service line growth, M&A, infusions of private equity capital, board interactions, and many of the firm's divisions. Mr. Friedberg was an officer and director of the firm, and a member of the compensation committee.

Before building Stroz Friedberg, Mr. Friedberg was for 11 years a federal prosecutor at the U.S. Attorney's Office in Brooklyn, New York. There, he was the head of the Narcotics Unit and the office's cybercrime practice. His most prominent case was the investigation, prosecution and conviction of six accomplices who assassinated a former editor of the New York City Spanish daily newspaper El Diario on orders of the Cali Cartel. For his leadership of the case, Mr. Friedberg received the 1994 Department of Justice Award for Superior Performance. In the cyber arena, Mr. Friedberg investigated and prosecuted cases involving hacking, denial of service attacks, malicious viruses, illegal data wiretapping and cyber-extortion.

Mr. Friedberg began his career as an intellectual property and securities litigator at Skadden, Arps.

Cyber Solutions Contacts

Jason J. Hogg
Chief Executive Officer
jason.j.hogg@aon.com

Eric Friedberg
Co-President
eric.friedberg@aon.com
+1 212.981.6536

Edward Stroz
Co-President
edward.stroz2@aon.com
+1 212.981.6541

Thomas E. Abel
Global Growth Officer
thomas.abel@aon com
+1 212.903.2818

AMERICAS

Christian E. Hoffman
President
christian.hoffman@aon.com
+1 212.441.2263

Stephanie Snyder
Commercial Strategy Leader
stephanie.snyder@aon.com
+1 312.381.5078

Chad Pinson
Executive Vice President Engagement Management — Cyber Security
chad.pinson@aon.com
+1 214.377.4553

CJ Dietzman
Managing Director
cj.dietzman@aon.com
+ 1 212.903.2828

Brian Rosenbaum
Senior Vice President
brian.rosenbaum@aon.ca
+1 416.868.2411

LATAM

Temo Garcia
Senior Broker & U.S./
Latin America Cyber Champion
temo.garcia@aon.com
+1 312.381.4398

EMEA

Onno Janssen
Chief Executive Officer
onno.janssen@aon.com
+49 (4) 03.605.3608

Richard Hanlon
Chief Commercial Officer
richard.hanlon@aon.ie
+353 1 266.6443

APAC

Michael Parrant
Cyber Insurance Practice Leader
michael.j.parrant@aon.com
+6 (141) 333.9783

Andrew Mahony
Regional Director
andrew.mahony@aon.com
+6 (58) 428.1965

Chris McLaughlin
Director
chris.mclaughlin@aon.com
+61 29253.7792

About Cyber Solutions

Aon's Cyber Solutions offers holistic cyber risk management, unsurpassed investigative skills and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets and recover from cyber incidents.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

Visit aon.com/cyber-solutions for more information.

Empower Results®