Board Level and Executive Reporting
How the Proposed SEC Cybersecurity Guidelines Will Impact Us

Demetrios Lazarikos (Laz)
Co-Founder and President, Blue Lava
laz@bluelava.io
Agenda

- Introductions
- Goals for today’s session
- SEC impact on reporting
- Gentle reminder on risk
- Recommendations
- Resources
Demetrios Lazarikos (Laz)

- A recognized authority for creating information security, fraud, and big data solutions
- 3x CISO
- Co-founder and President, Blue Lava
- 30+ years experience across several verticals
  - Orbitz
  - Sears
  - SilverTail
  - NewEdge Financial / Société Générale
  - vArmour
  - United States Air Force (USAF)
- Undergrad:
  - Colorado State University
- Graduate:
  - Masters in Computer Security, University of Denver
  - MBA: Pepperdine University
BLUE LAVA
With, by, and for the greater security community
https://community.bluelava.io
Advising leadership on the future

Skillfully partnering, advising, and influencing senior leadership on the future while adapting to business and regulatory requirements.
Advising leadership on the future
Skillfully partnering, advising, and influencing senior leadership on the future while adapting to business and regulatory requirements

Understanding impact
How the new SEC proposals for Cybersecurity disclosure may impact us and our security programs
Advising leadership on the future
Skillfully partnering, advising, and influencing senior leadership on the future while adapting to business and regulatory requirements

Understanding impact
How the new SEC proposals for Cybersecurity disclosure may impact us and our security programs

Communicating cybersecurity
Effectively communicate security program within your organization while navigating business risk, systemic risk, and transformation
Research & Statistics
Security Program Management: Priorities and Strategies

A peer survey of practices and goals for measuring and managing security programs and communicating priorities to executives and boards

- How often they communicate with the board of directors?
- The challenges they face managing security activities and developing roadmaps?
- The impact of clearly communicating security priorities and investments to executive management?

268 CISOs, CIOs, senior security and risk managers
www.bluelava.io
Blue Lava Security Program Management Survey

Is communicating security priorities and needs a challenge?

- Strongly agree: 31.0%
- Somewhat agree: 41.8%
- Somewhat disagree: 16.0%
- Strongly disagree: 11.2%

SOURCE: Blue Lava and AimPoint Group Report
Security Program Management: Priorities and Strategies
Top-Third-Performing CISOs’ Proposed Changes in Time Allocation
Average Hours Overinvested or Underinvested per 50-Hour Workweek

- Security Operations: 1.5 hours per week overinvested
- Staff Management: 1.2 hours per week overinvested
- Policy and Standards Setting: 0.7 hours per week overinvested
- Project Risk Assessment and Oversight: 0.5 hours per week overinvested
- Vendor Management: 0.3 hours per week overinvested

Effective CISOs want to invest more time in strategic planning and building relationships.

n = 129 CISOs
Source: 2020 Gartner CISO Effectiveness Survey

728433_C
Digital Transformation and Cyber Security Predictions
Predictions

60% of the global GDP will be digitized and 70% of new value created in the economy over the next decade will be based on digitally enhanced platforms.

– World Economic Forum, 2022

Over the past three decades, $20 has been added to the GDP for every $1 invested in digital technologies. This is 6.7x the rate for non-digital investments.

– Oxford Economics, 2017

Research shows that emerging digital ecosystems could account for more than $60 trillion in revenue by 2025 (or more than 30% of global corporate revenue), and yet only 3% of established companies have adopted an active platform strategy.

– World Economic Forum, 2022

Cybercrime will cost the global economy $10.5 trillion annually by 2025 making cybercrime equivalent to the third largest economy in the world - right behind the US and China.

– Cybercrime Magazine, November 2020
SEC Impact on Cybersecurity Decisions
SEC Proposed Cybersecurity Guidelines and Reporting

- Incident reporting in 8-K within four days (if material)
- Security program management
- Board oversight for cybersecurity risk with expertise at the board level
- Cybersecurity expertise within the company
Sarbanes-Oxley Lessons Learned

- 2000 (20 years ago)
- Corporate boards to have a director in the room who understood a financial statement

- In 2003, 21% of Boards reported having a financial expert
  - ~146 financial experts in total
- By 2012, 100% of the S&P 500 boards report having at least one financial expert
  - ~1,096 financial experts in total
Comparing Career Tracks

Finance career track
Comparing Career Tracks

Finance career track
CISO career track
The Evolution of Digital & Systemic Risk
Cyber risk and digital transformation
Exponential adoption of new technology in support of business growth has outpaced the ability to secure it, resulting in systemic cyber risk.

Applying a wider industry lens
Businesses in similar vertical markets or industries leverage technology in similar ways, therefore sharing common security business risks.

Reporting on your business
You must understand the uniqueness of your own business’ technical landscape to determine your most critical security business risks.
Educate the Board and Executives Now!
## Cyber Risk has Grown Exponentially

### Evolution of Technology

<table>
<thead>
<tr>
<th>Year</th>
<th>Device</th>
<th>Applications</th>
<th>Data</th>
<th>Speed</th>
<th>Social Media</th>
<th>Perimeter</th>
<th>Hackers</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>Desktop/Laptop</td>
<td>Client/Server</td>
<td>1 Exabyte</td>
<td>2G</td>
<td>Instant Messenger</td>
<td>Controlled Access</td>
<td>Script Kiddies</td>
<td>Intrusive</td>
</tr>
<tr>
<td>2007</td>
<td>Mobile</td>
<td>Web</td>
<td>1/4 Zettabyte</td>
<td>3G</td>
<td>Facebook</td>
<td>Wide Access</td>
<td>Criminal Ecosystem</td>
<td>Disruptive</td>
</tr>
<tr>
<td>2014</td>
<td>IoT (Internet of Things)</td>
<td>Agile</td>
<td>1 Zettabyte</td>
<td>4G</td>
<td>Twitter</td>
<td>Hybrid Cloud</td>
<td>Hactivists</td>
<td>Destructive</td>
</tr>
<tr>
<td>2021</td>
<td>IoE (Internet of Everything)</td>
<td>Automation</td>
<td>100 Zettabytes</td>
<td>5G</td>
<td>TikTok, Instagram</td>
<td>No Perimeter</td>
<td>Other Non-state Actors (Terrorists?)</td>
<td>Cyber Armageddon?</td>
</tr>
</tbody>
</table>

### Risk

- **2000**: Intrusive
- **2007**: Disruptive
- **2014**: Destructive
- **2021**: Cyber Armageddon?
Evolving Security Models

2000

REACTIVE

- Perimeter
- Static
- Siloed

2010

INTELLIGENCE DRIVEN

- Risk-Based
- Dynamic
- Leveraged

2020

OPERATION-CENTRIC

- Dynamic Risk
- AI/ML Driven
- Ops Focused
Evolution of Smart Products and Systems
Evolution of Smart Products and Systems

- Product
- Smarter Product
- Smarter Connected Product
- Product Integration System
Evolution of the Medical Device
Evolution of the Medical Device

1
Product

2
Smarter Product
Evolution of the Medical Device

1  Product
2  Smarter Product
3  Smarter Connected Product
### Evolution of the Medical Device

<table>
<thead>
<tr>
<th></th>
<th>Product</th>
<th>Smarter Product</th>
<th>Smarter Connected Product</th>
<th>Health Integrated System</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Medical Integrated System

- Monitoring/Alerting
  - Status
  - Rate
  - 911

- Medical Management System
  - Health Integrated System
  - Order Entry / Fulfillment
  - M.D. Portal Integration
  - Bidirectional Communication w/ Stakeholders

- Support
  - Individual
  - Provider
  - Insurance
Evolution of the Automobile

1. Product
2. Smarter Product
3. Smarter Connected Product
4. Automobile Intergrated System
The Automobile Integrated System

- Trip Planner
- Weather
- Research
- Gas Station
- Auto Mechanic
- Insurance
- Shopping Carts
- Social Media
- Ad Sensors
Automobile System of Systems
Evolution of the Home
The Home Integrated System

- Monitoring
- Home Integrated System
- Home Management System
- Maintenance
- Shopping
  - Online Security
  - Physical Security
  - Emergency Services
  - Parts
  - Utilities
  - Insurance
  - Ad Sensors
  - Wish Lists
  - Streaming Movies
Interconnected System of Systems

Blue Lava, Inc.
SEC Proposed Cybersecurity Guidelines and Reporting

- Incident reporting in 8-K within four days (if material)
- Security program management
- Board oversight for cybersecurity risk with expertise at the board level
- Cybersecurity expertise within the company
SEC Proposed Cybersecurity Guidelines Overview

- The SEC is suggesting a new approach to cybersecurity disclosure and reporting
  - [https://www.sec.gov/rules/proposed/2022/33-11038.pdf](https://www.sec.gov/rules/proposed/2022/33-11038.pdf)
- This new approach is suggesting required amendments for reporting in the following areas:
  - Disclose cyber incidents in their 8-K within four days of deeming it material
  - Disclose policies, procedures, security program management, and risk assessments for managing risks from cyber threats
  - Disclose the Board's mechanisms for cyber risk oversight
  - Disclose cyber expertise within the company
SEC Proposed Cybersecurity Guidelines Overview

8K Reporting

- A new item (1.05) added to Form 8-K. As is the case with almost all other Form 8-K items, 1.05 would:
  - Require companies to disclose material cybersecurity incidents within four business days
  - The trigger date for the disclosure is the date of the materiality determination - NOT - the date of discovery of the incident
  - Required disclosure would include:
    - Incident discovery - and - if it is ongoing
    - A brief description of nature/scope of the incident
    - If data was stolen, altered, accessed, or used for any other unauthorized purpose
    - The effect of the incident on the company's operations
    - Whether the company has remediated (or is currently remediating the incident)
SEC Proposed Cybersecurity Guidelines Overview | Program Management

- Proposed Item 106(b) would therefore require registrants to disclose its policies and procedures, if it has any, to identify and manage cybersecurity risks and threats, including, but not limited to:
  - Operational risk
  - Intellectual property theft
  - Fraud
  - Extortion
SEC Proposed Cybersecurity Guidelines Overview | Program Management

- Proposed Item 106(b) would therefore require registrants to disclose its policies and procedures, if it has any, to identify and manage cybersecurity risks and threats, including, but not limited to:
  - Operational risk
  - Intellectual property theft
  - Fraud
  - Extortion

- **Security Program Management**
  - The registrant has a cybersecurity risk assessment program and if so, provide a description of such program;
  - The registrant engages assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program;
  - The registrant has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third-party service provider (including, but not limited to, those providers that have access to the registrant’s customer and employee data).
SEC Proposed Cybersecurity Guidelines Overview | Program Management

- Proposed Item 106(b) would therefore require registrants to disclose its policies and procedures, if it has any, to identify and manage cybersecurity risks and threats, including, but not limited to:
  - Operational risk
  - Intellectual property theft
  - Fraud
  - Extortion

- **Security Program Management**
  - The registrant has a cybersecurity **risk assessment program** and if so, provide a description of such program
  - The registrant **engages assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program**
  - The registrant has **policies and procedures** to oversee and **identify the cybersecurity risks** associated with its use of any **third-party service provider** (including, but not limited to, those providers that have access to the registrant’s customer and employee data)

- **Monitoring/Alerting/Incidents**
  - The registrant **undertakes activities to prevent, detect, and minimize effects of cybersecurity incidents**
  - The registrant has **business continuity, contingency, and recovery** plans in the event of a cybersecurity incident
  - **Previous cybersecurity incidents** have informed changes in the registrant’s governance, policies and procedures, or technologies
  - Cybersecurity related risk and incidents have affected or are reasonably likely to affect the registrant’s results of **operations or financial condition** and if so, how cybersecurity risks are considered as part of the registrant’s business strategy, financial planning, and capital allocation and if so, how
SEC Proposed Cybersecurity Guidelines Overview | Internal Expertise

- Specifically, as it pertains to the board’s oversight of cybersecurity risk, disclosure required by proposed Item 106(c)(1) would include a discussion, as applicable, of the following:
  - Whether the entire board, specific board members or a board committee is responsible for the oversight of cybersecurity risks;
  - Whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight
SEC Proposed Cybersecurity Guidelines Overview | Internal Expertise

- Specifically, as it pertains to the board’s oversight of cybersecurity risk, disclosure required by proposed Item 106(c)(1) would include a discussion, as applicable, of the following:
  - Whether the entire board, specific board members or a board committee is responsible for the oversight of cybersecurity risks;
  - Whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight

- Qualified and Trained Personnel
  - Whether the registrant has a designated chief information security officer, or someone in a comparable position, and if so, to whom that individual reports within the registrant’s organizational chart (and experience)
  - Whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, specifically the prevention, mitigation, detection, and remediation of cybersecurity incidents, and the relevant expertise of such persons or members
  - Frequency of this person reporting to the board of directors or a committee of the board of directors on cybersecurity risk
SEC Proposed Cybersecurity Guidelines Overview | Board Expertise

- Specifically, as it pertains to the board’s oversight of cybersecurity risk, disclosure required to amend Item 407 of Regulation S-K by adding paragraph (j) to require:
  - Disclosure about the **cybersecurity expertise of members of the board** of directors of the registrant, if any.
  - If any **member of the board has cybersecurity expertise**, the registrant would have to disclose the name(s) of any such director(s), and provide such detail as necessary to fully describe the nature of the expertise.
SEC Proposed Cybersecurity Guidelines Overview | Board Expertise

- Specifically, as it pertains to the board’s oversight of cybersecurity risk, disclosure required to amend Item 407 of Regulation S-K by adding paragraph (j) to require:
  - Disclosure about the **cybersecurity expertise of members of the board** of directors of the registrant, if any.
  - If any **member of the board has cybersecurity expertise**, the registrant would have to disclose the name(s) of any such director(s), and provide such detail as necessary to fully describe the nature of the expertise.

- Qualified and Trained Personnel
  - Whether the **director has prior work experience in cybersecurity**, including, for example, prior experience as an **information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager, or business continuity planner**
  - Whether the **director has obtained a certification or degree in cybersecurity**
  - Whether the **director has knowledge, skills, or other background in cybersecurity**, including, for example, in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling, or business continuity planning
Reporting
# A Board Calendar for US Public Companies

<table>
<thead>
<tr>
<th></th>
<th>Full Board</th>
<th>Audit Committee</th>
<th>Comp Committee</th>
<th>Corp Gov</th>
</tr>
</thead>
<tbody>
<tr>
<td>January</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>February</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>March</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April</td>
<td>X (Phone)</td>
<td>X (Phone)</td>
<td>X (Phone)</td>
<td>X (Phone)</td>
</tr>
<tr>
<td>May</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>June</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>August</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>September (Retreat)</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>October</td>
<td></td>
<td></td>
<td>X (Phone)</td>
<td></td>
</tr>
<tr>
<td>November</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>December</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Source: Sydley Austin, LLP and DDN
# A Board Calendar for US Public Companies

<table>
<thead>
<tr>
<th></th>
<th>Full Board</th>
<th>Audit Committee</th>
<th>Comp Committee</th>
<th>Corp Gov</th>
<th>Cyber Committee</th>
</tr>
</thead>
<tbody>
<tr>
<td>January</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>February</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>March</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April</td>
<td>X (Phone)</td>
<td>X (Phone)</td>
<td>X (Phone)</td>
<td>X (Phone)</td>
<td>X (Phone)</td>
</tr>
<tr>
<td>May</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>June</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>August</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>September</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>(Retreat)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>October</td>
<td></td>
<td>X (Phone)</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>November</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>December</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Source: Sydley Austin, LLP and DDN

**Recommended Structure**
- NOT Under Audit/IT Audit
- Separate Cyber Committee
- Led by the CISO
Where we are
Board of Directors Cybersecurity Update

Security program maturity score and targets

- Targets: Q3 2021, Q4 2021, Q1 2022
- Scores: 1.58, 2.11, 2.45, 3.25

Visual representation of maturity scale:
- Ad hoc
- Current
- Visionary

Top 5 security risks and progress made against them

1. Ability to recover from ransomware: Identified key business recovery requirements
2. Protecting apps against malicious attackers: Implemented secure coding practices
3. Data management & protection: Made data flow diagrams mapping sensitive data
4. Protecting the network: More comprehensive vulnerability patching
5. Security awareness: Annual security training now includes phishing
Where we are
Board of Directors Cybersecurity Update

Risk and Peer Benchmarking

Top 5 security risks and progress made against them

- Ability to recover from ransomware
  - Identified key business recovery requirements
- Protecting apps against malicious attackers
  - Implemented secure coding practices
- Data management & protection
  - Made data flow diagrams mapping sensitive data
- Protecting the network
  - More comprehensive vulnerability patching
- Security awareness
  - Annual security training now includes phishing
Recommendations
PREPARING FOR THE SEC PROPOSED GUIDELINES

Recommendations

Relationships and Accountability
Build, educate, and nurture relationships with internal and external key business partners now

Data
Evaluate whether or not you have the data and systems you need to report

Communication & Reporting
Examine if you’re effectively communicating and reporting clearly & consistently
Resources

● San Diego ISACA
  ○ [https://isaca-sd.org/](https://isaca-sd.org/)
● The SEC Proposed Cybersecurity Guidelines
● Blue Lava AimPoint Survey
● SEC Webinar Prep Discussions
  ○ Part 1 - Understanding the Impact
  ○ Part 2 - What Now
  ○ Part 3 - Impact on my Career
Thank You!

Demetrios Lazarikos (Laz)
Co-Founder and President, Blue Lava
laz@bluelava.io

https://community.bluelava.io