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

ISACA® San Diego Chapter

BLUELAVA

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

BLUELAVA

With, by, and for the
greater security community

https://community.bluelava.io

Actionable Goals for Today's Session

Advising leadership on the future

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

Actionable Goals for Today’s Session

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

Actionable Goals for Today's Session

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

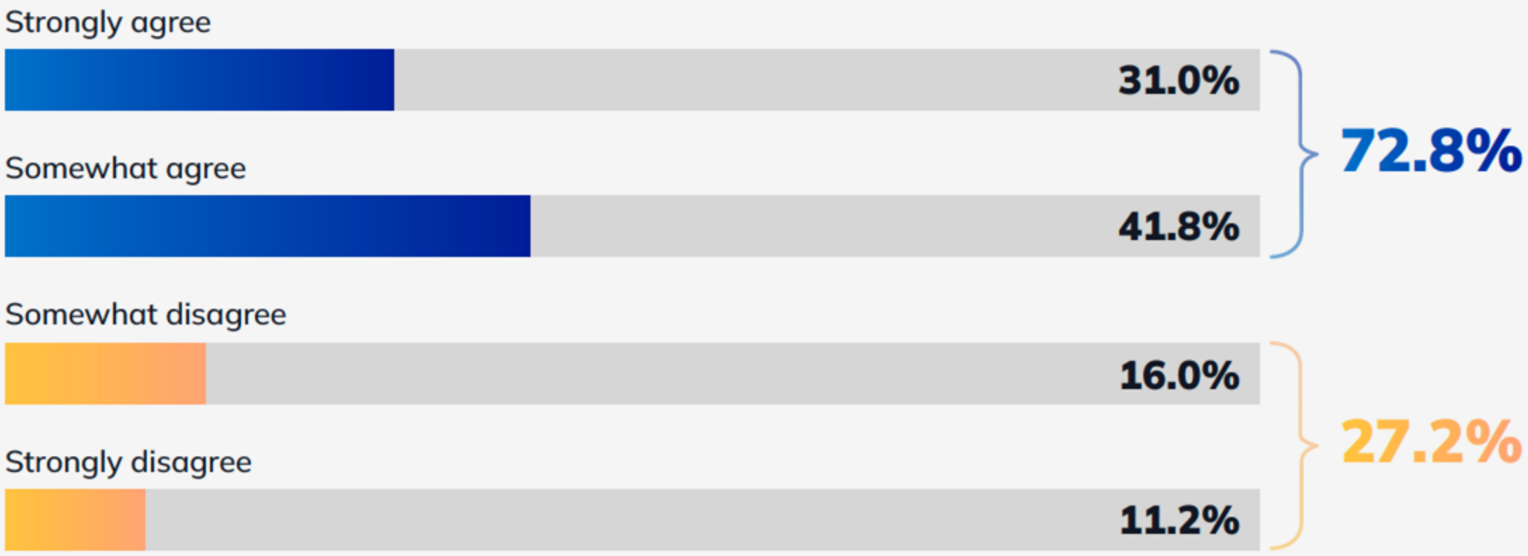
A peer survey of practices and goals for measuring and managing security programs and communicating priorities to executives and boards

- 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

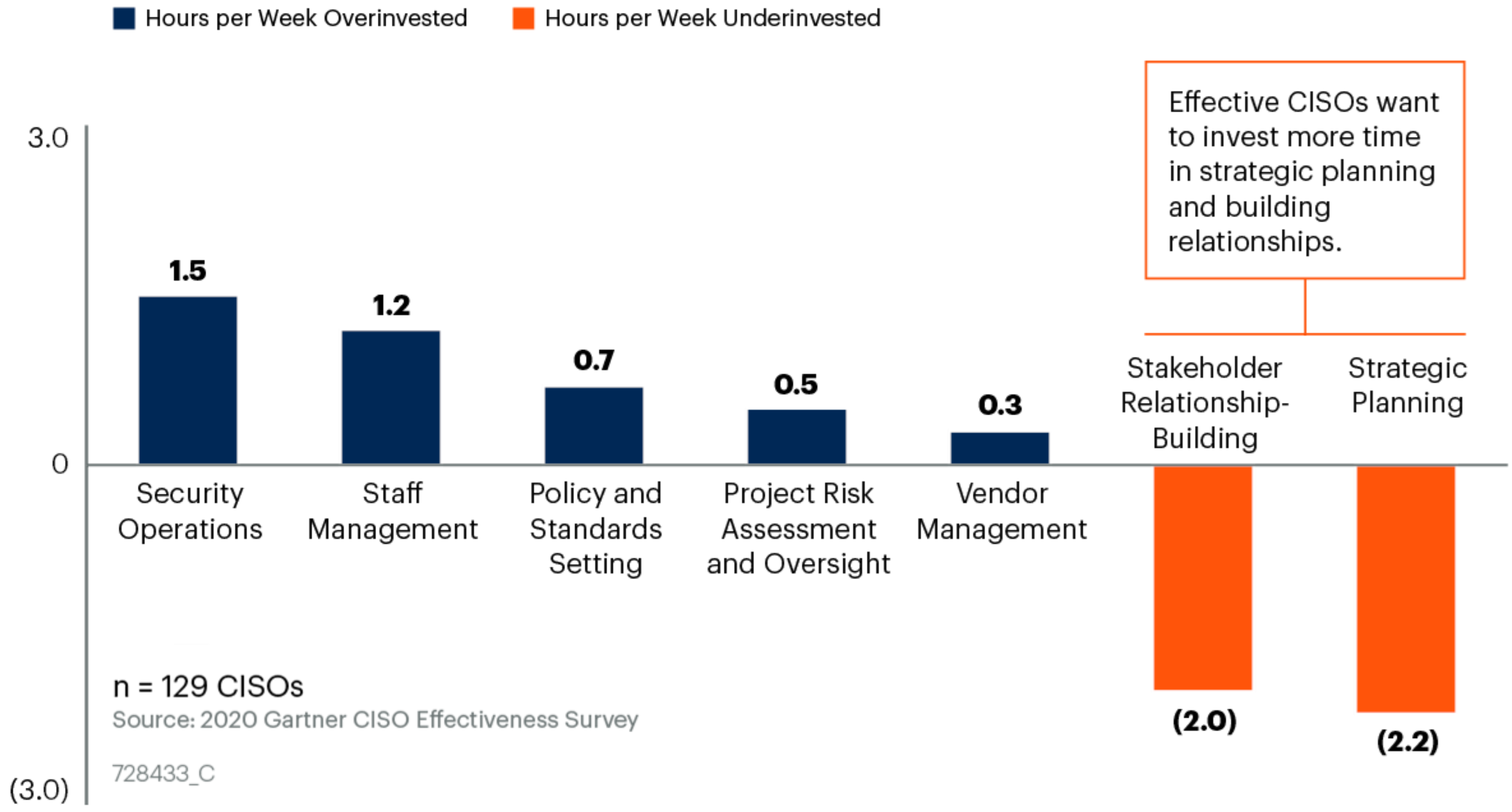
Is communicating security priorities and needs a challenge?



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



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

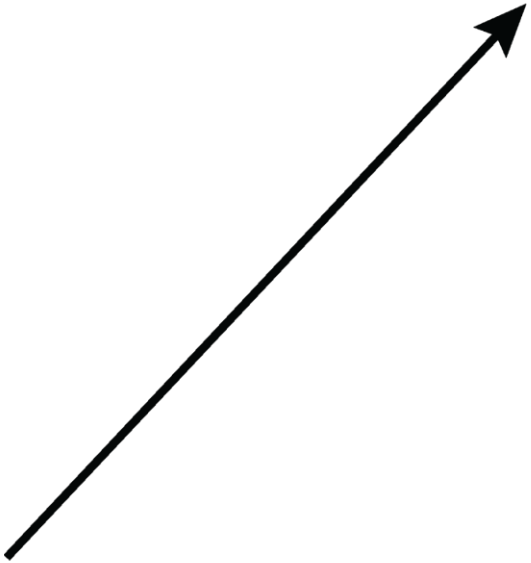
- Incident reporting in 8-K within four days (if material)
- Security program management
- Board oversight for cybersecurity risk with expertise at the board level
- Cybersecurity expertise within the company

Sarbanes-Oxley Lessons Learned

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

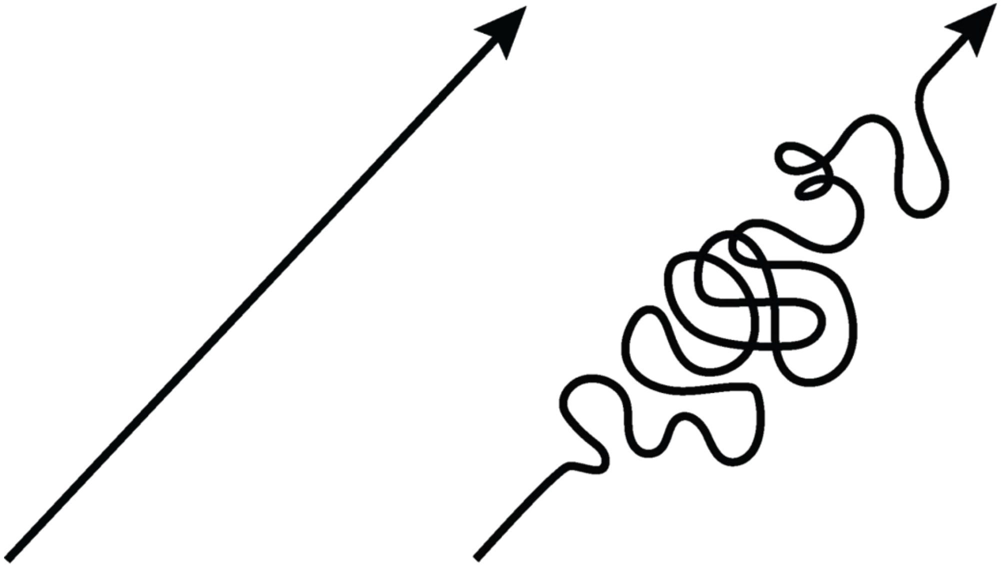
- In 2003, 21% of Boards reported having a financial expert
  - ~146 financial experts in total
- By 2012, 100% of the S&P 500 boards report having at least one financial expert
  - ~1,096 financial experts in total

Comparing Career Tracks



Finance career track

Comparing Career Tracks



Finance career track

CISO career track

The Evolution of Digital & Systemic Risk

Mapping the Business to Your Cybersecurity Program

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

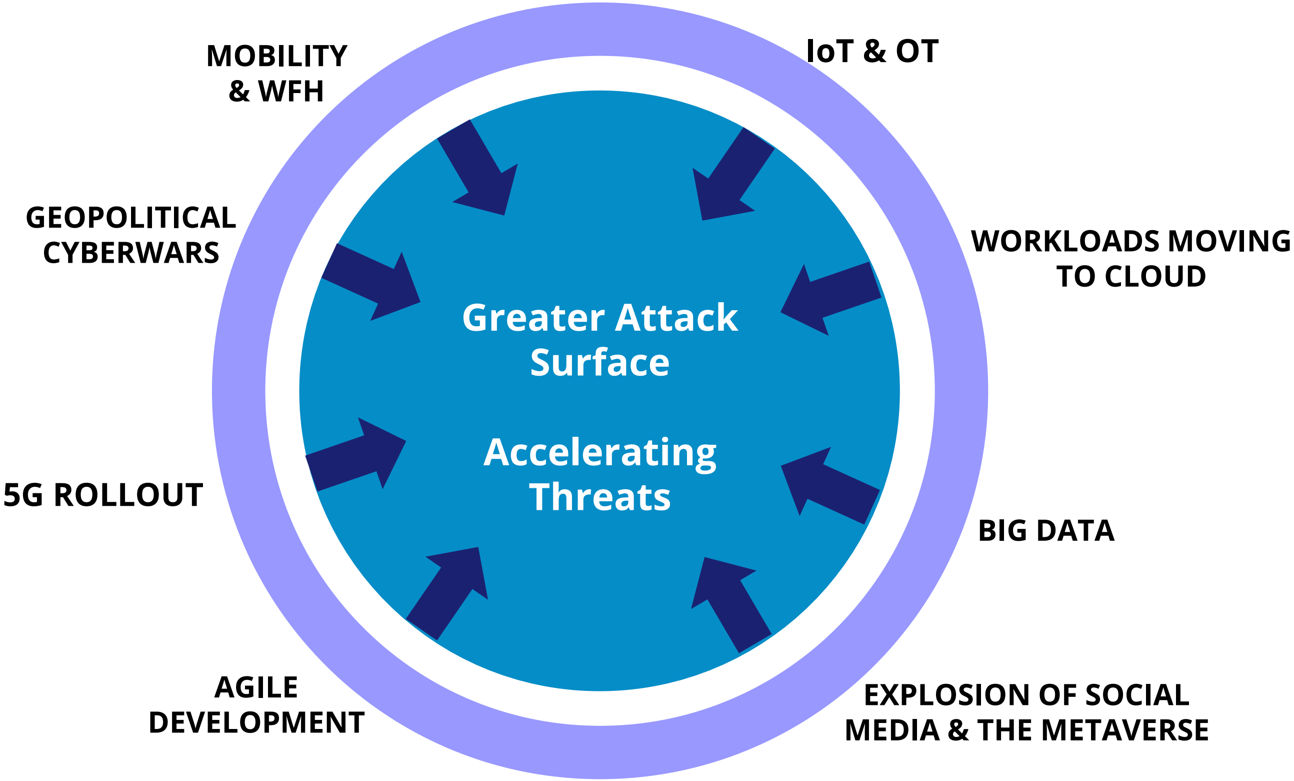
You must understand the uniqueness of your own business' technical landscape to determine your most critical security business risks.

Educate the Board and Executives Now!

Cyber Risk has Grown Exponentially

	2000	2007	2014	2021
DEVICE	Desktop/Laptop	Mobile	IoT (Internet of Things)	IoE (Internet of Everything)
APPLICATIONS	Client/Server	Web	Agile	Automation
DATA	1 Exabyte	1/4 Zettabyte	1 Zettabyte	100 Zettabytes
SPEED	2G	3G	4G	5G
SOCIAL MEDIA	Instant Messenger	Facebook	Twitter	TikTok, Instagram
PERIMETER	Controlled Access	Wide Access	Hybrid Cloud	No Perimeter
HACKERS	Script Kiddies	Criminal Ecosystem	Hactivists	Other Non-state Actors (Terrorists?)
ATTACKS	Intrusive	Disruptive	Destructive	Cyber Armageddon?

The Next 20 Years



Evolving Security Models

2000

REACTIVE

Perimeter
Static
Siloed

2010

INTELLIGENCE DRIVEN

Risk-Based
Dynamic
Leveraged

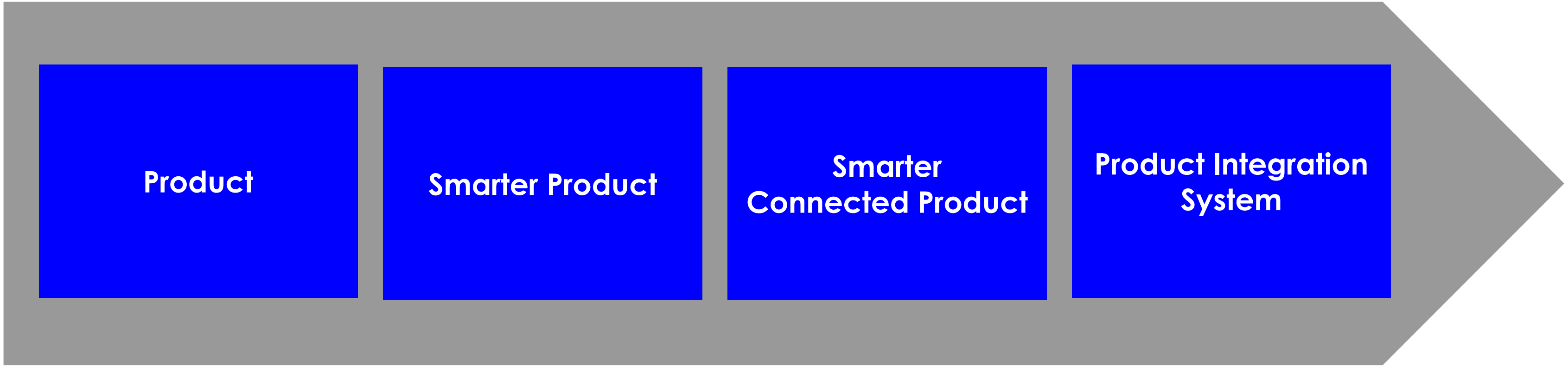
2020

OPERATION-CENTRIC

Dynamic Risk
AI/ML Driven
Ops Focused

Evolution of Smart Products and Systems

Evolution of Smart Products and Systems



Product

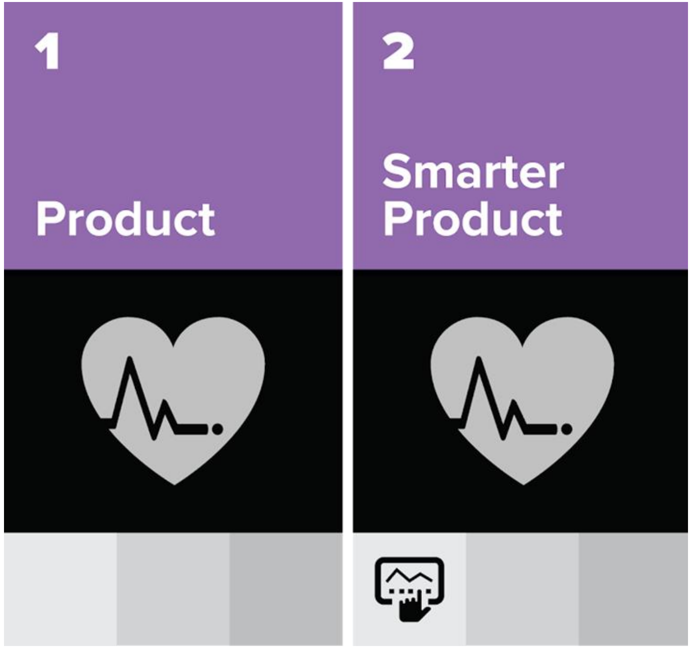
Smarter Product

Smarter Connected Product

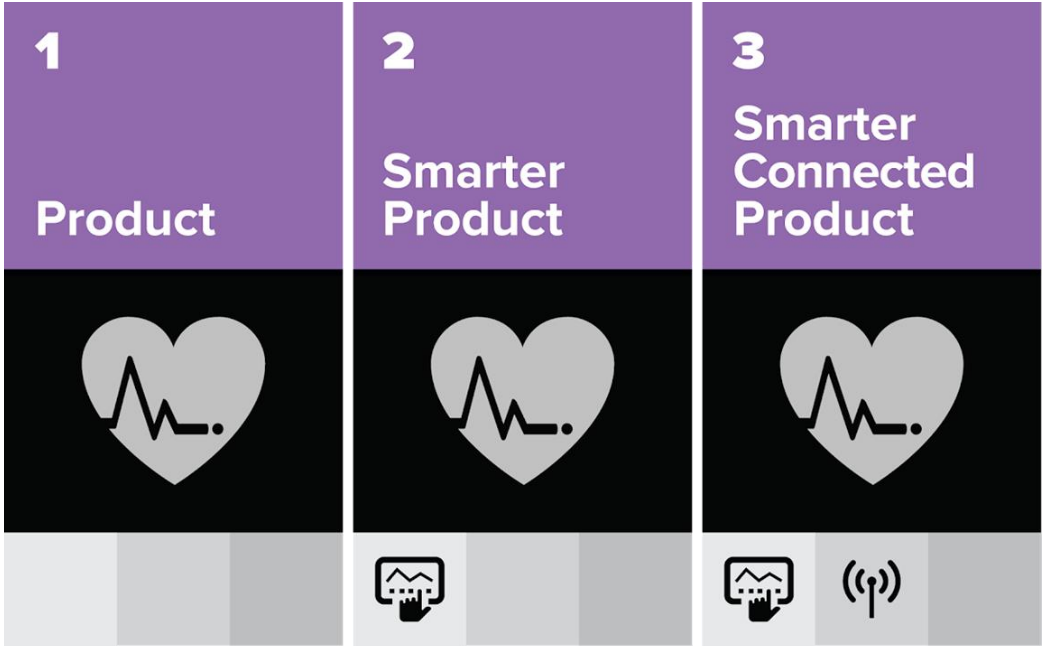
Product Integration System

Evolution of the Medical Device

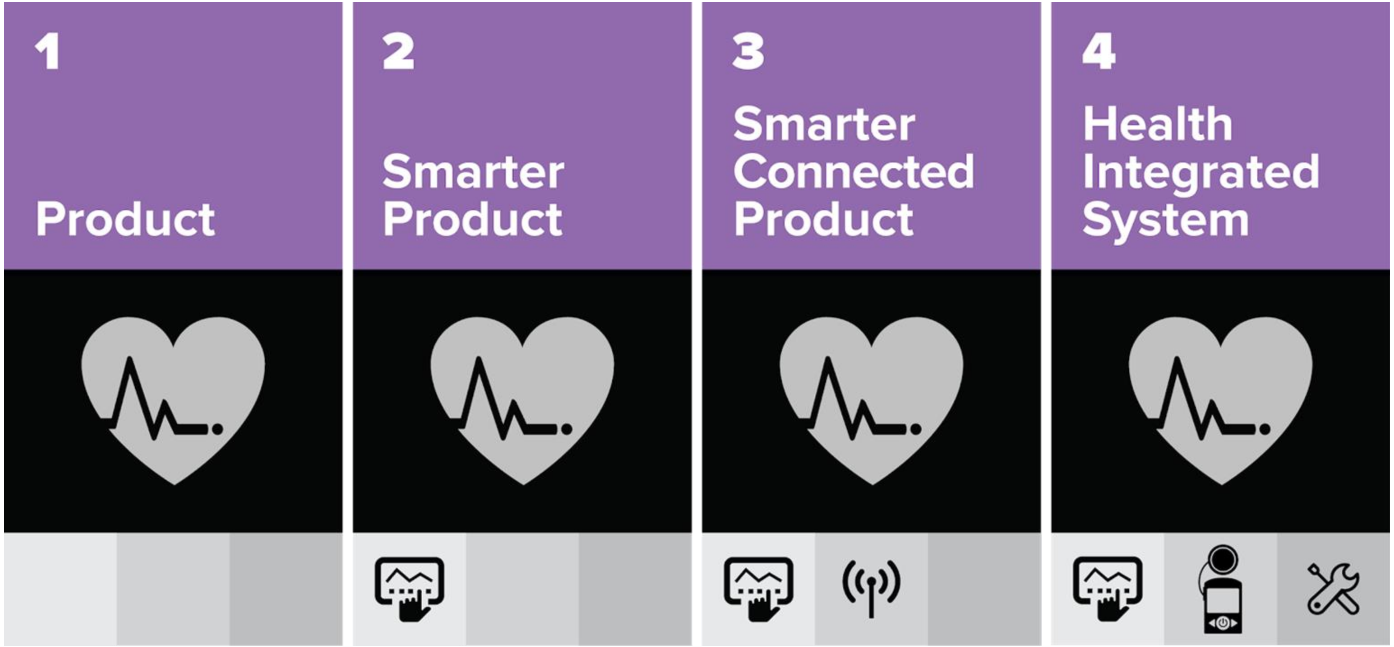
Evolution of the Medical Device



Evolution of the Medical Device



Evolution of the Medical Device



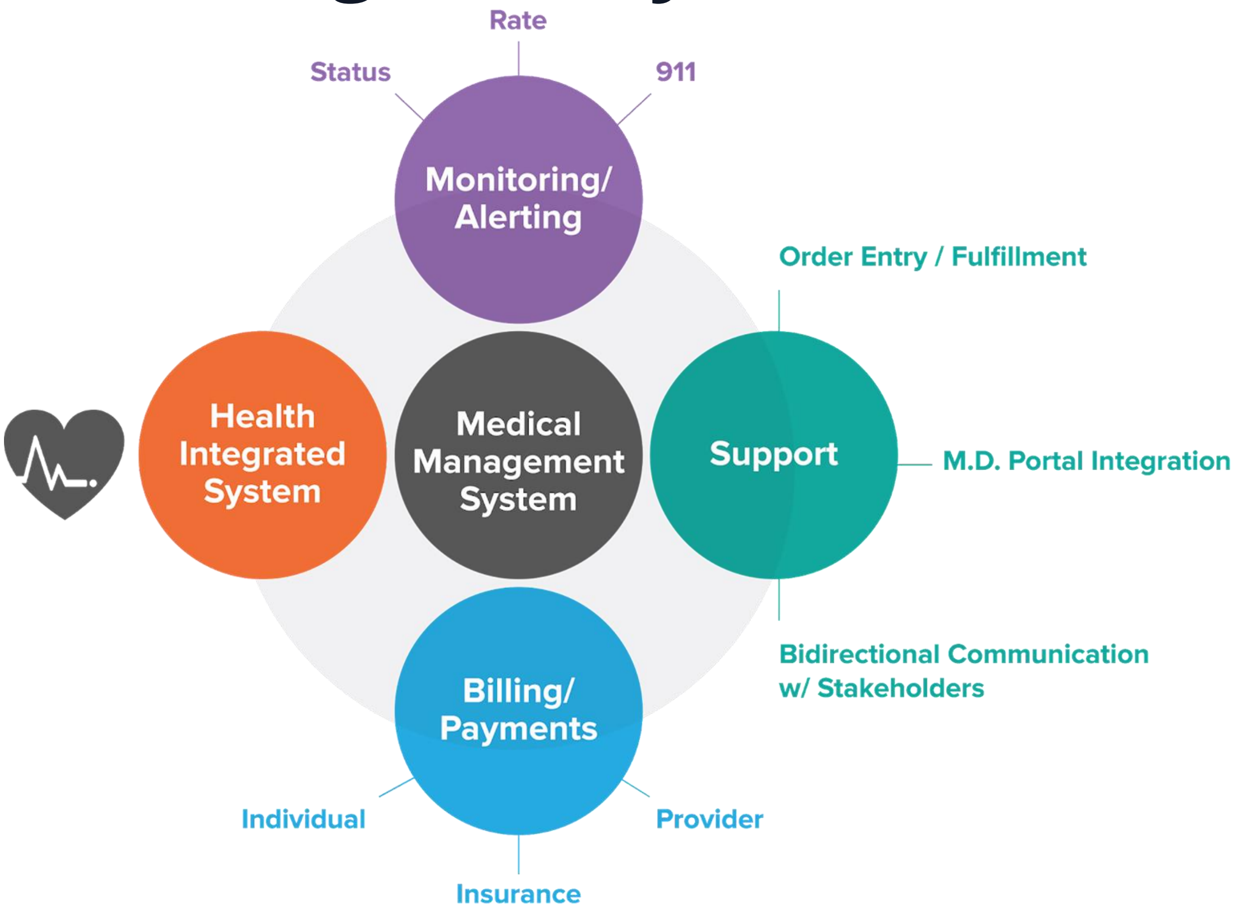
1 Product

2 Smarter Product

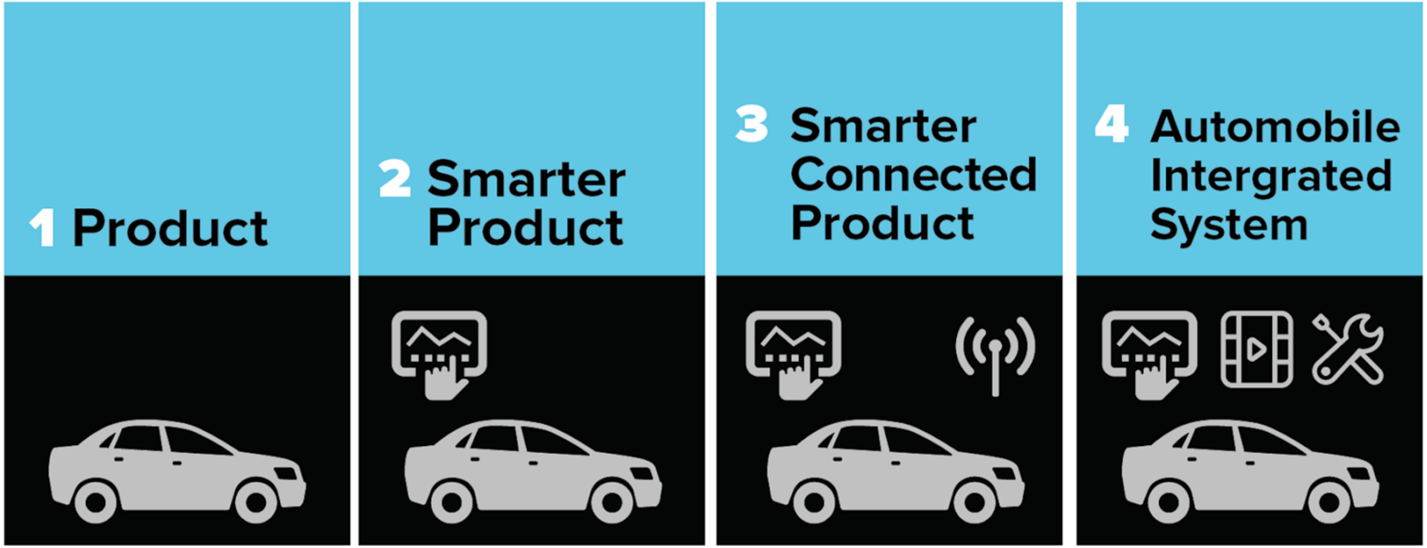
3 Smarter Connected Product

4 Health Integrated System

The Medical Integrated System



Evolution of the Automobile



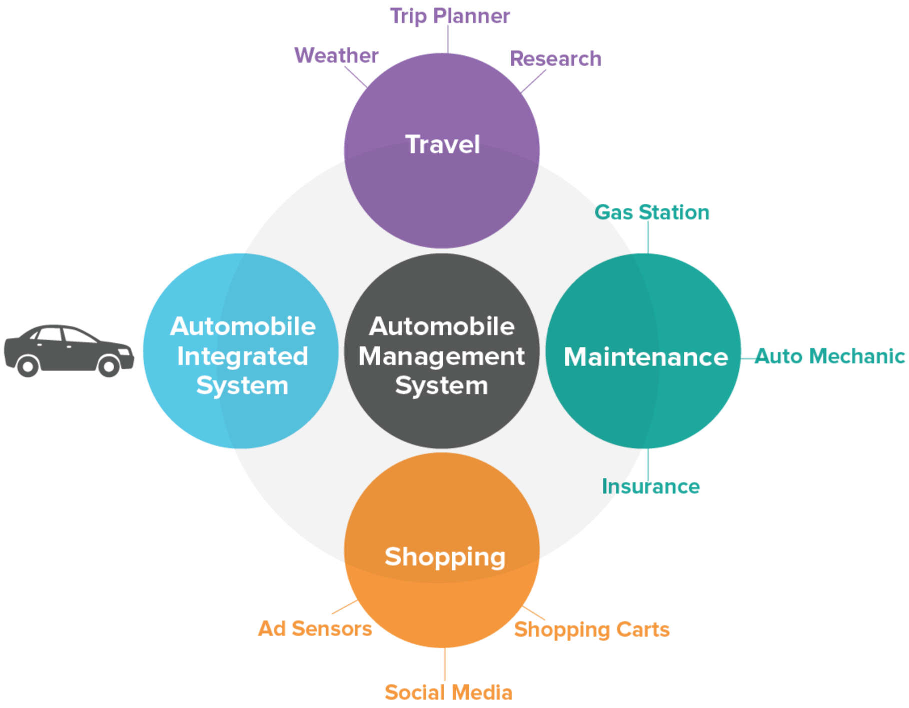
1 Product

2 Smarter Product

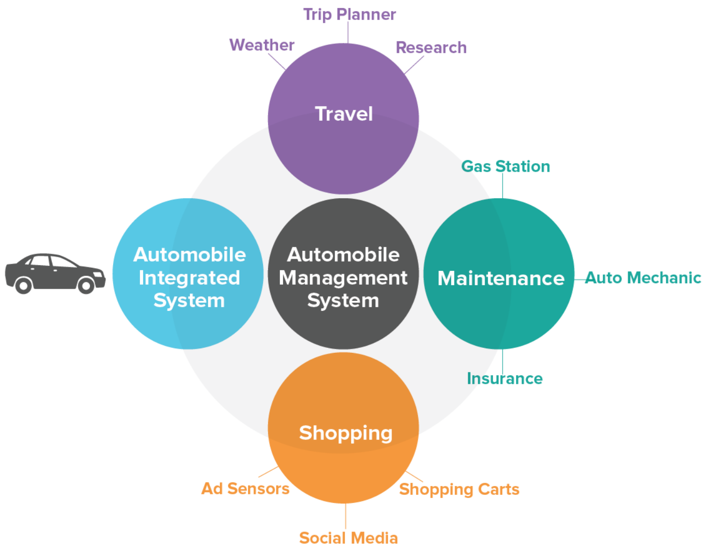
3 Smarter Connected Product

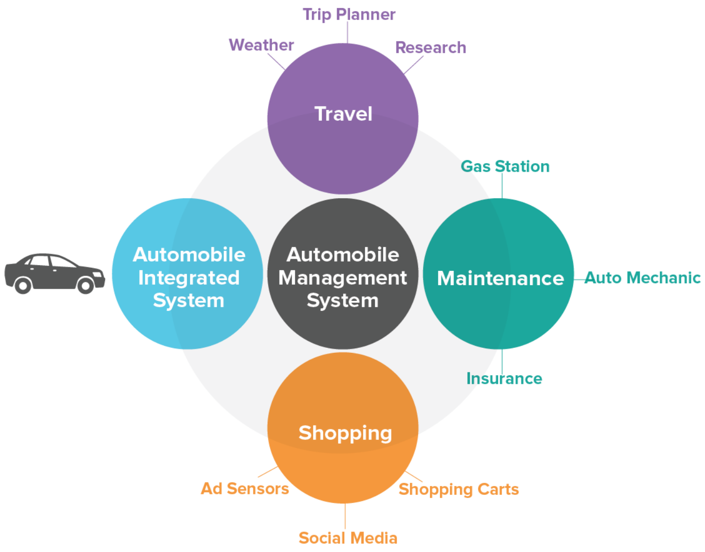
4 Automobile Intergrated System

The Automobile Integrated System

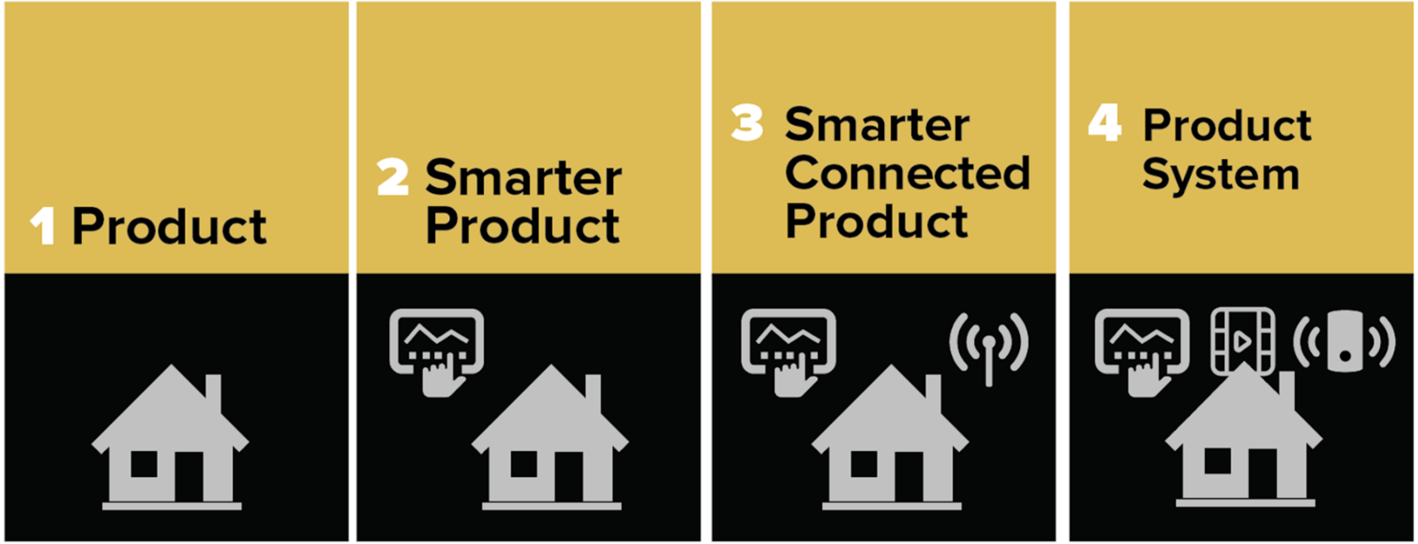


Automobile System of Systems





Evolution of the Home



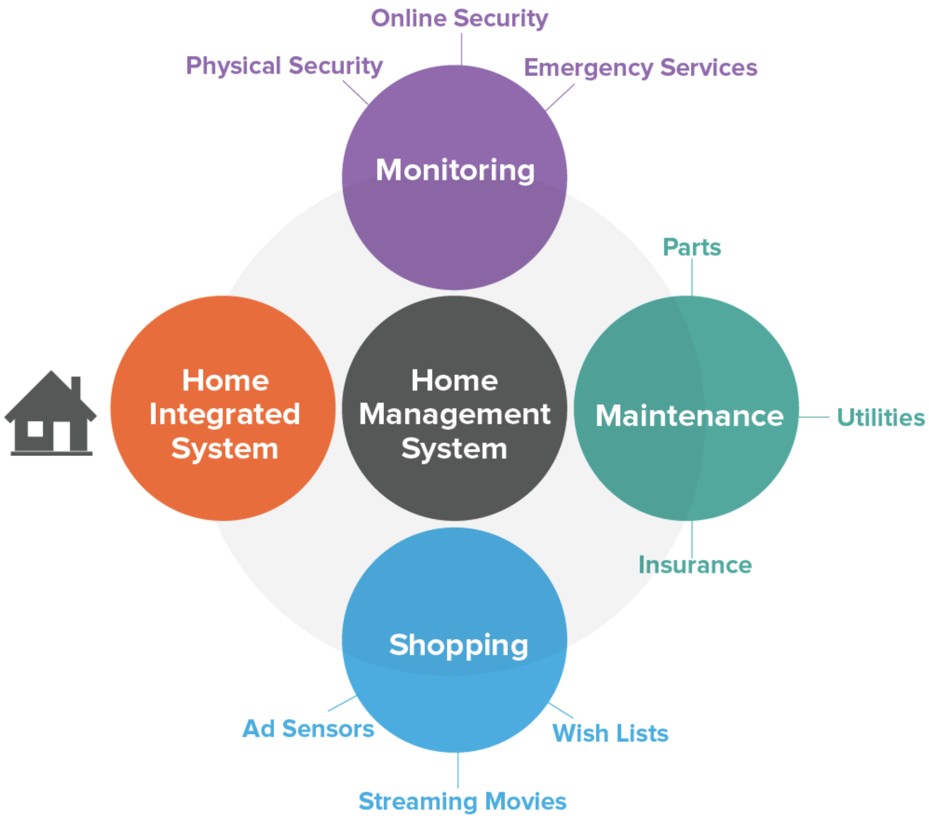
1 Product

2 Smarter Product

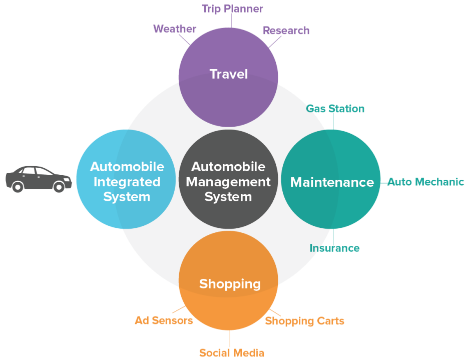
3 Smarter Connected Product

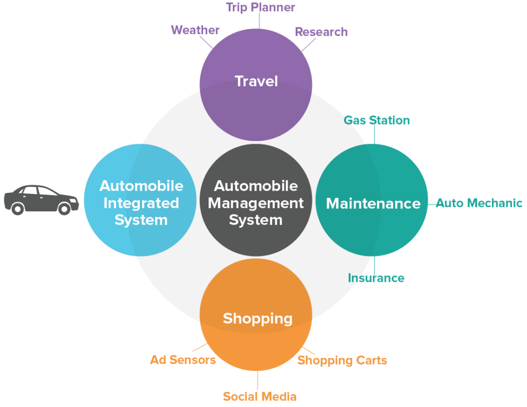
4 Product System

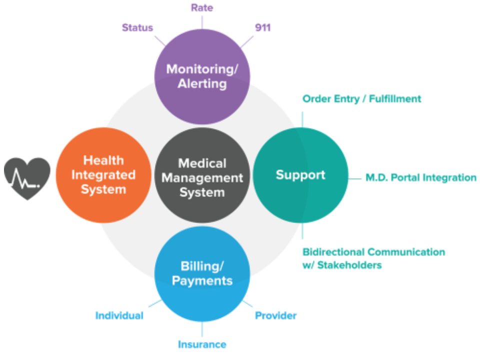
The Home Integrated System

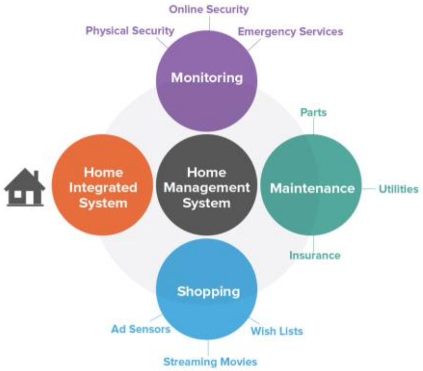


Interconnected System of Systems









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
- 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 i**dentify 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 i**dentify 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

STEP BY STEP

A Board Calendar for US Public Companies

	Full Board	Audit Committee	Comp Committee	Corp Gov
January	X	X	X	X
February	X	X	X	
March				
April	X (Phone)	X (Phone)	X (Phone)	X (Phone)
May	X	X		
June				
July	X	X	X	X
August				
September (Retreat)	X			X
October		X (Phone)		
November	X		X	
December		X		

Source: Sydley Austin, LLP and DDN

STEP BY STEP

A Board Calendar for US Public Companies

Recommended Structure

- NOT Under Audit/IT Audit
- Separate Cyber Committee
- Led by the CISO

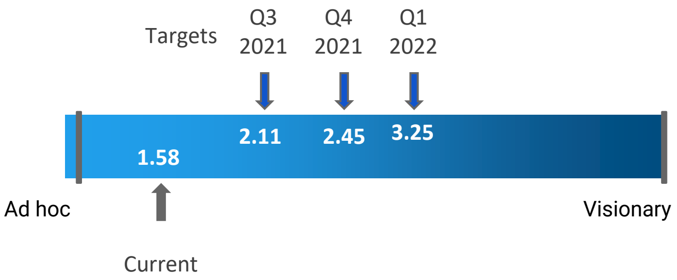
	Full Board	Audit Committee	Comp Committee	Corp Gov	Cyber Committee
January	X	X	X	X	X
February	X	X	X		X
March					
April	X (Phone)	X (Phone)	X (Phone)	X (Phone)	X (Phone)
May	X	X			
June					
July	X	X	X	X	X
August					
September (Retreat)	X			X	X
October		X (Phone)			
November	X		X		X
December		X			

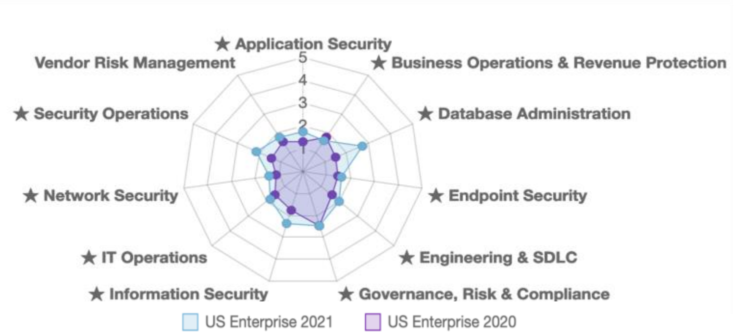
Source: Sydley Austin, LLP and DDN

Where we are

Board of Directors Cybersecurity Update

Security program maturity score and targets





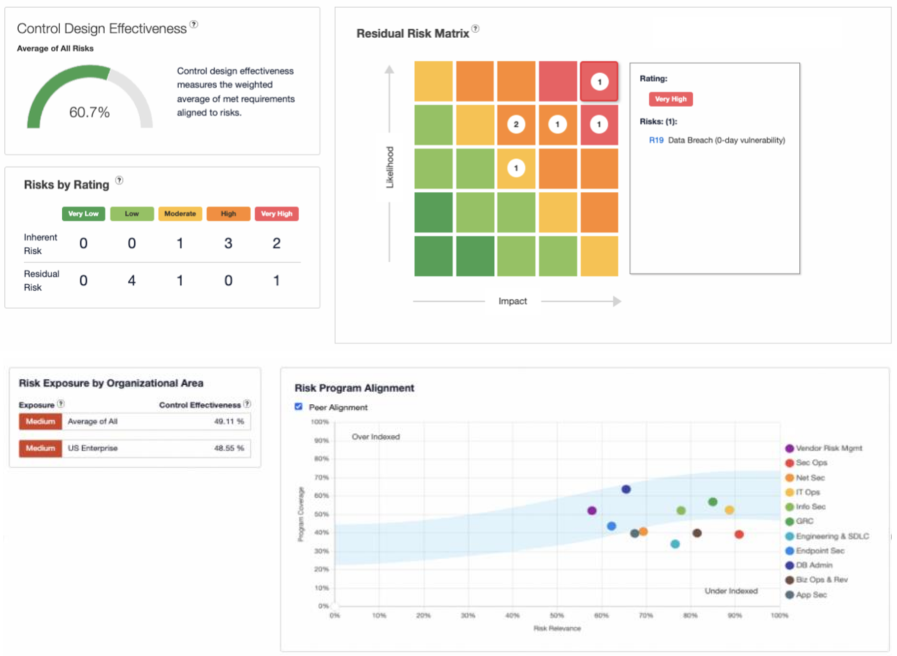
Top 5 security risks and progress made against them

Ability to recover from ransomware	Identified key business recovery requirements
Protecting apps agains 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

Where we are

Board of Directors Cybersecurity Update

Risk and Peer Benchmarking



Control Design Effectiveness

Average of All Risks

60.7%

Control design effectiveness measures the weighted average of met requirements aligned to risks.

Risks by Rating

	Very Low	Low	Moderate	High	Very High
Inherent Risk	0	0	1	3	2
Residual Risk	0	4	1	0	1

Residual Risk Matrix

Rating: Very High

Risks: (1):

R19 Data Breach (0-day vulnerability)

Risk Exposure by Organizational Area

Exposure		Control Effectiveness
Medium	Average of All	49.11 %
Medium	US Enterprise	48.55 %

Risk Program Alignment

☑ Peer Alignment

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

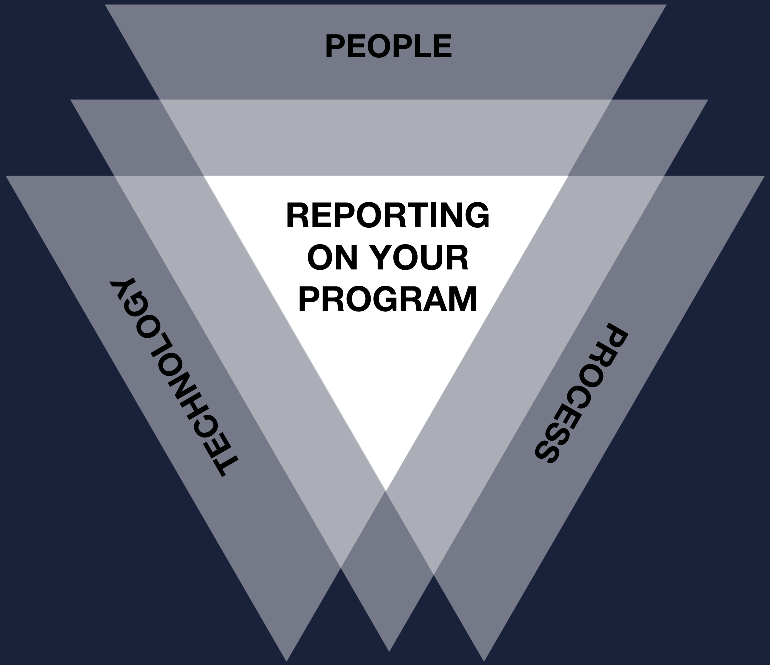
Build, educate, and nurture relationships with internal and external key business partners now

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/
- **The SEC Proposed Cybersecurity Guidelines**
  - https://www.sec.gov/rules/proposed/2022/33-11038.pdf
- **Blue Lava AimPoint Survey**
  - https://bluelava.io/security-program-management-priorities-and-strategies/
- **SEC Webinar Prep Discussions**
  - **Part 1 - Understanding the Impact**
    - https://info.bluelava.io/webinar-part-one-sec-guidelines
  - **Part 2 - What Now**
    - https://info.bluelava.io/webinar-part-two-sec-guidelines
  - **Part 3 - Impact on my Career**
    - https://info.bluelava.io/webinar-part-three-sec-guidelines
- **CISO Evolution | ISBN-13: 978-1119782483 | ISBN-10: 1119782481**
- **If It's Smart, It's Vulnerable 1st Edition | ISBN-10: 1119895189 | ISBN-13: 978-1119895183**
- **The Great Reboot: Succeeding in a Complex Digital World Under Attack From Systemic Risk | ISBN-10 : 173504301X | ISBN-13 : 978-1735043012**

Thank You!

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

https://community.bluelava.io

BLUELAVA