# Cybersecurity Strategy Under the Microscope

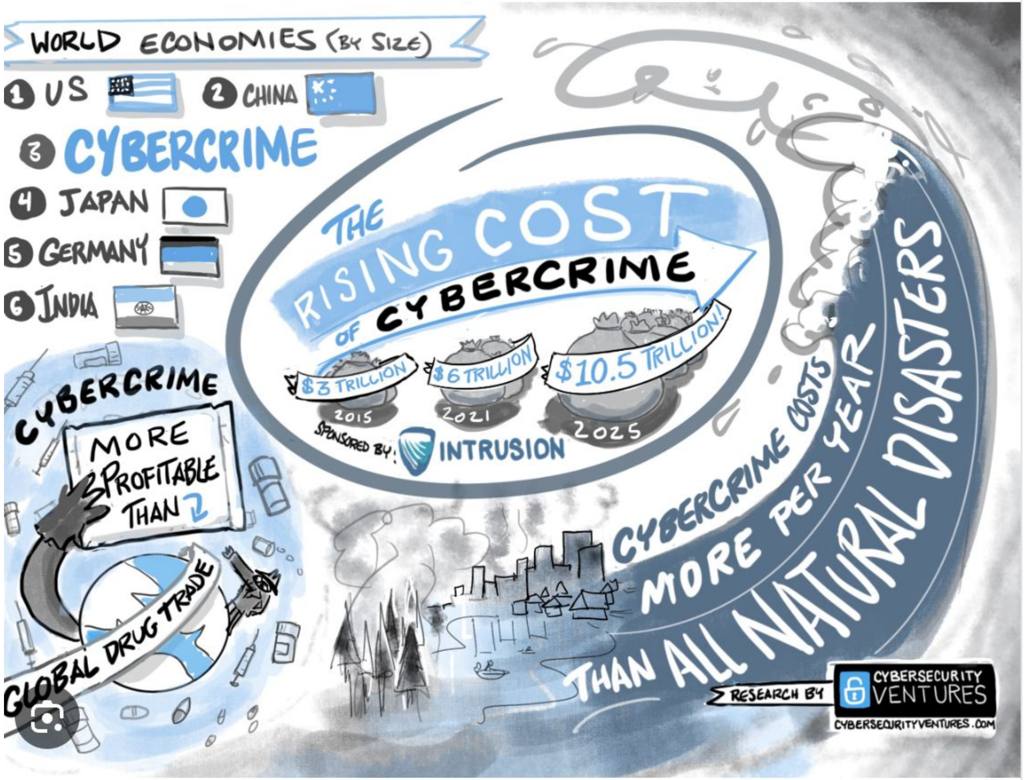
## *Cyber Program Effectiveness is the new Benchmark!*

Vishal Chawla, Katie Reilly

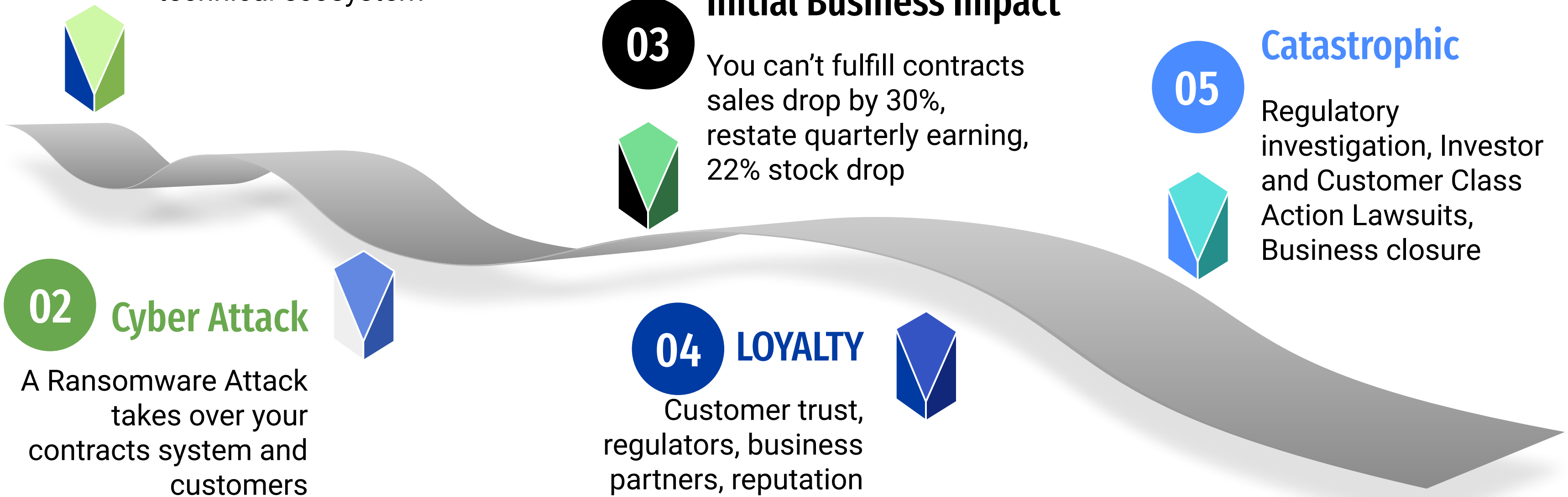
NY Metro Joint Cyber Security Conference, 24

BLUOCEAN

# Cybercrime is costlier than natural disasters


WORLD ECONOMIES (BY SIZE)
1 US
2 CHINA
3 CYBERCRIME
4 JAPAN
5 GERMANY
6 INDIA
THE RISING COST OF CYBERCRIME
$3 TRILLION
2015
$6 TRILLION
2021
$10.5 TRILLION!
2025
SPONSORED BY: INTRUSION
CYBERCRIME MORE PROFITABLE THAN
GLOBAL DRUG TRADE
CYBERCRIME COSTS MORE PER YEAR THAN ALL NATURAL DISASTERS
RESEARCH BY CYBERSECURITY VENTURES
CYBERSECURITYVENTURES.COM

# Cyber criminals are focusing on disrupting business operations



01 **Cyber Breach**

Criminal gets into your technical ecosystem

02 **Cyber Attack**

A Ransomware Attack takes over your contracts system and customers information.

03 **Initial Business Impact**

You can’t fulfill contracts sales drop by 30%, restate quarterly earning, 22% stock drop

04 **LOYALTY**

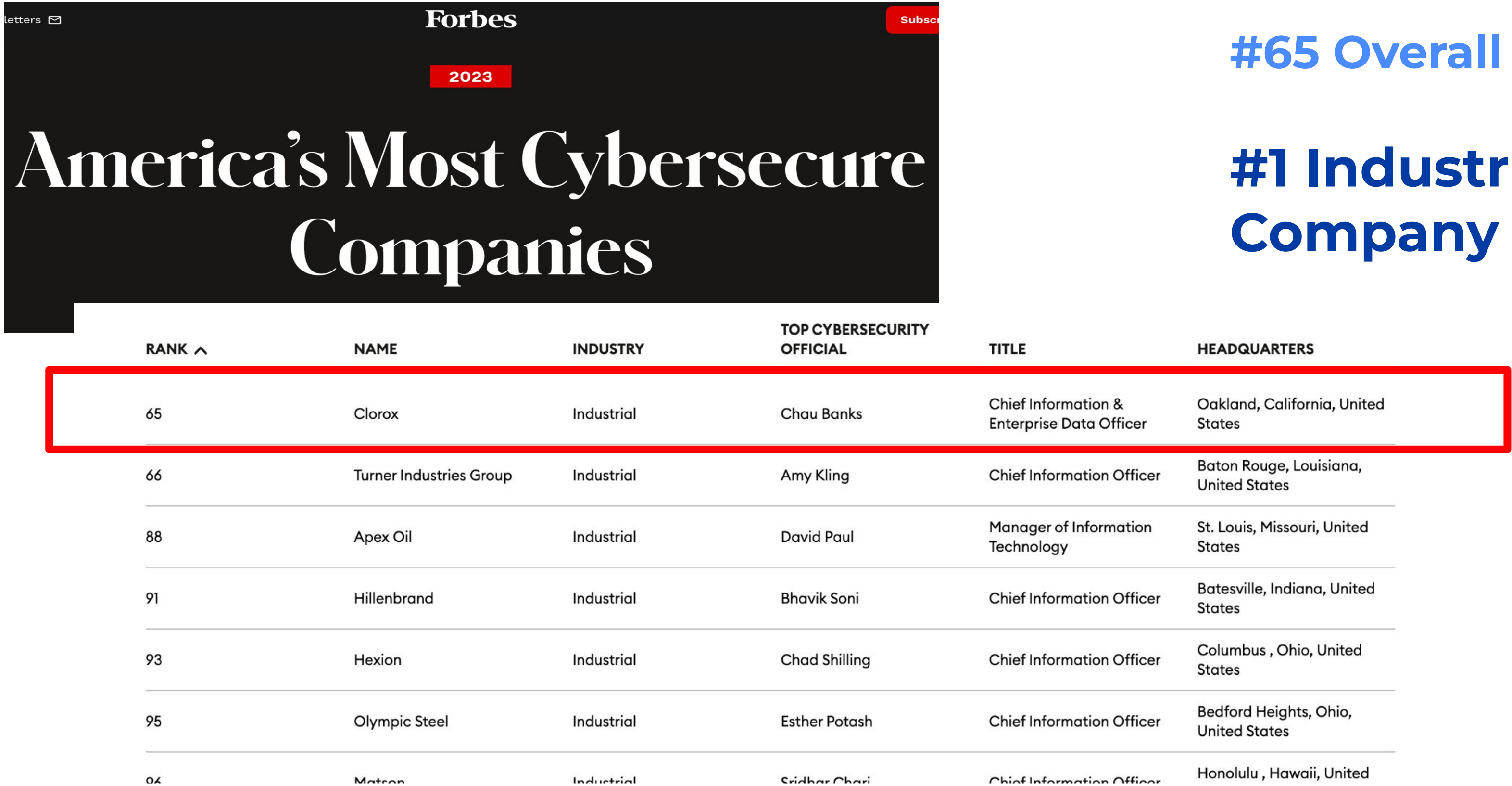
Customer trust, regulators, business partners, reputation impact

05 **Catastrophic**

Regulatory investigation, Investor and Customer Class Action Lawsuits, Business closure

# Case Study: Clorox Disruption Attack

# June 2023: Clorox on Top of Security List!



letters Forbes Subscr

2023

America's Most Cybersecure Companies

| RANK ^ | NAME | INDUSTRY | TOP CYBERSECURITY OFFICIAL | TITLE | HEADQUARTERS |
|---|---|---|---|---|---|
| 65 | Clorox | Industrial | Chau Banks | Chief Information & Enterprise Data Officer | Oakland, California, United States |
| 66 | Turner Industries Group | Industrial | Amy Kling | Chief Information Officer | Baton Rouge, Louisiana, United States |
| 88 | Apex Oil | Industrial | David Paul | Manager of Information Technology | St. Louis, Missouri, United States |
| 91 | Hillenbrand | Industrial | Bhavik Soni | Chief Information Officer | Batesville, Indiana, United States |
| 93 | Hexion | Industrial | Chad Shilling | Chief Information Officer | Columbus , Ohio, United States |
| 95 | Olympic Steel | Industrial | Esther Potash | Chief Information Officer | Bedford Heights, Ohio, United States |
| 96 | Matson | Industrial | Sridhar Chari | Chief Information Officer | Honolulu , Hawaii, United |

## #65 Overall

## #1 Industrial Company

# How do you get to the top of the security list?

“ Companies ranked by their website security and cybersecurity infrastructure”

In partnership with the research company SecurityScorecard

Rankings based on maturity scores!!

# August 2023: An SEC Filing

About the SEC

The mission of the SEC is to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation. The SEC strives to promote a market environment that is worthy of the public's trust.

SEC Proposed Rules

We encourage the public to submit comi comment period. For detailed instructio Proposed rules currently available inclu

**SEC filing stating "identified unauthorized activity " that is "expected to continue to disrupt parts of the Company's business operations."**

**Instead of targeting data, OT systems, or user endpoints, hackers attacked systems that disrupted Clorox's supply chain**

- **Cyber criminals took Purchase Order systems offline - including systems where large retailers like Walmart and Target order products**

# Breaking the Supply Chain

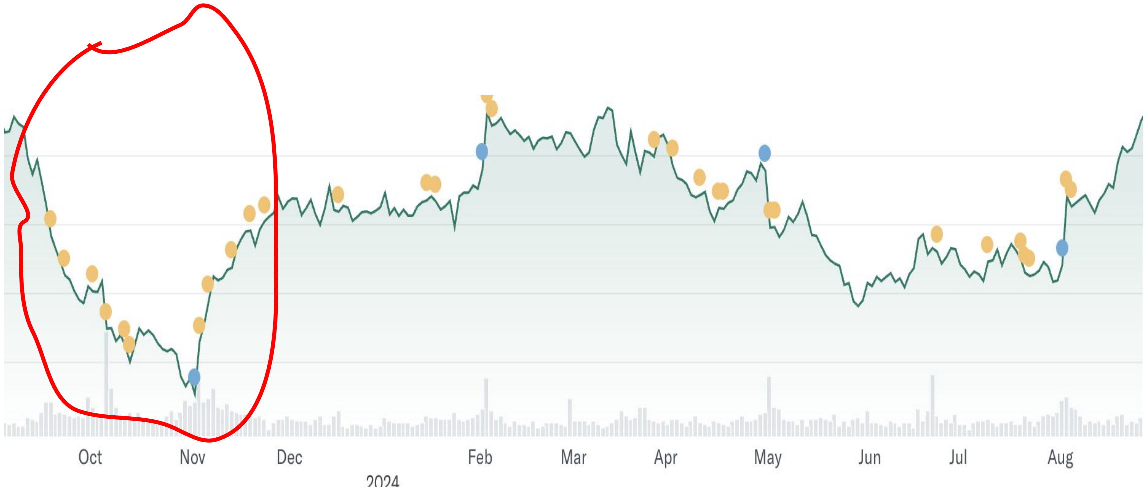
**Orders had to be processed manually**

**Orders drive the supply chain system, which in turn directs factory workloads—18 out of 23 factories reduced production to 50%.**

**Clorox had to go manual on many of its procedures**

**Operations slowed and shelves were left empty**

# September 2023: A Material Incident



**Another SEC filing "an elevated level of consumer product availability issues."**

**Predicted a loss of 23%-28% in net sales, loss of per share earning ranging from 35-to-75 cents, order processing delays, and "elevated level of product outages."**

**Stated this attack will be material on future financial results.**

# What Happens after a Material Incident?

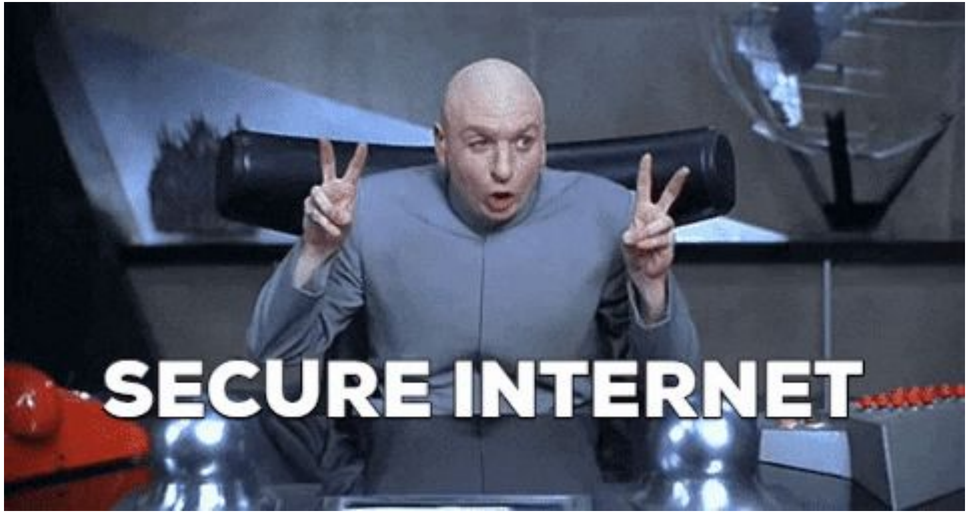
Order processing delays and significant product outages

$49 million in costs related to the attack by the end of 2023

Net sales were expected to decrease between $487-593 million

May 2024: After 9 months gained 90% of prior market share back

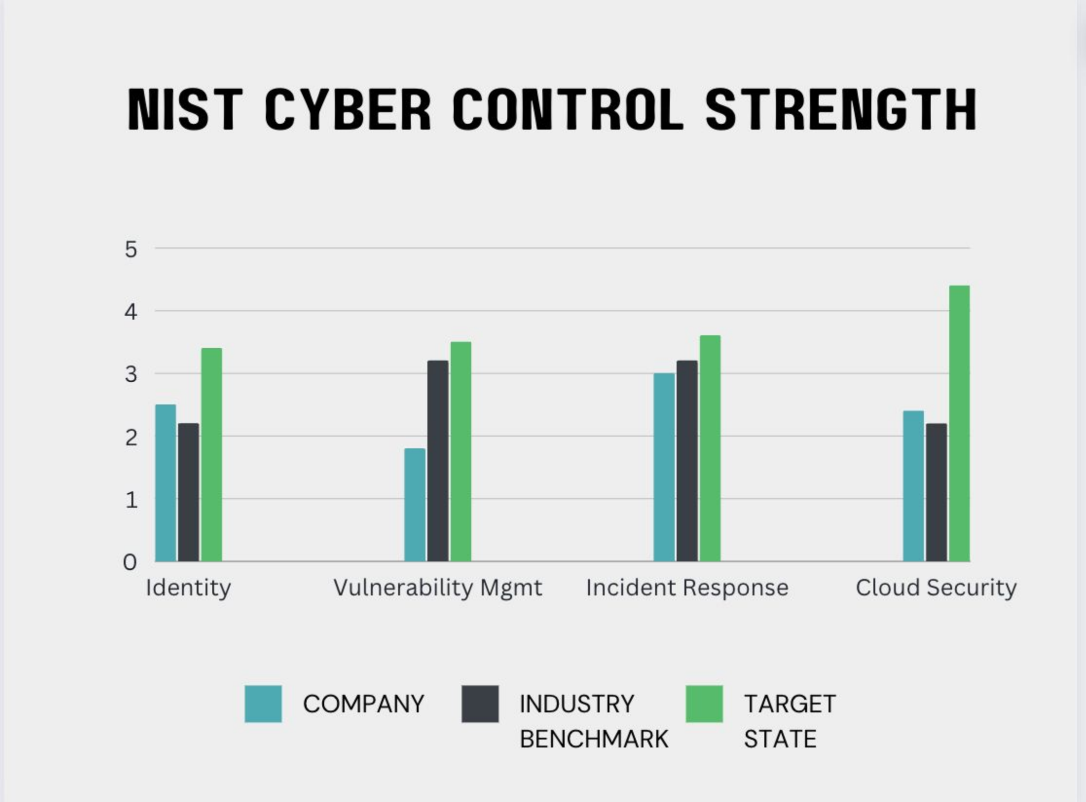
# Hackers don’t care about your good grades!



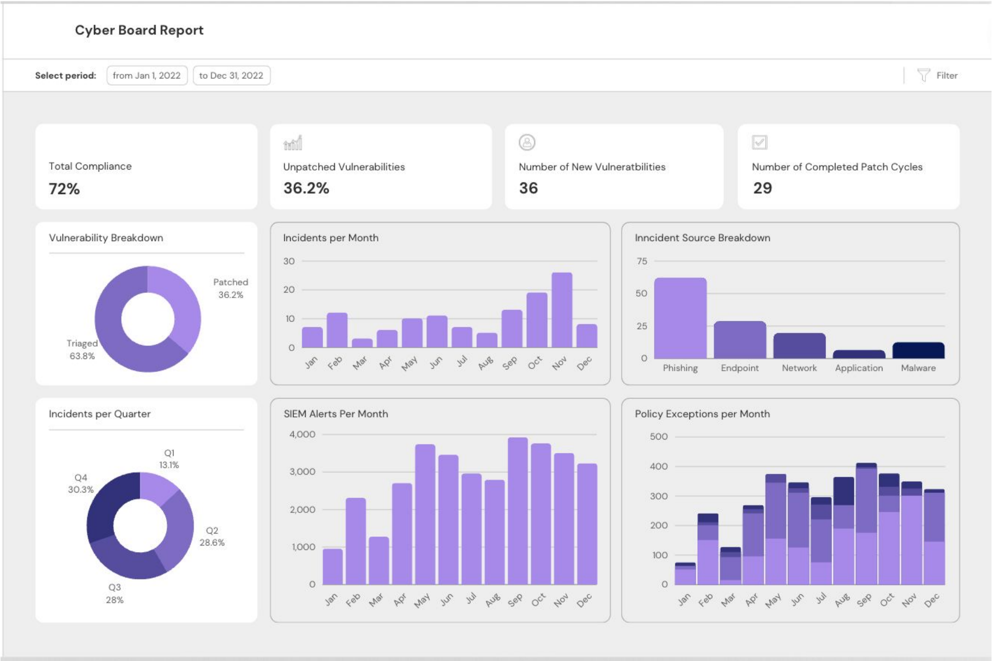
# Cyber maturity assessments do not prepare you for business disruption attacks

| The answers traditional cyber assessments provide | The answers that matter to your business and regulators |
|---|---|
| How mature are my controls for a NIST CSF category? | How well are my critical business processes protected by our cyber program? |
| Am I compliance with NIST, ISO, and PCI standards? | Have we defined what a material cyber incident would look like for the business? |
| What tools can I buy to increase my cyber maturity scores? | Can we demonstrate that cyber investments have been made to protect critical business processes? |

# Cyber maturity metrics have no business risk context or actionable insight



# And metrics with No meaning to Business!!



Cyber Board Report

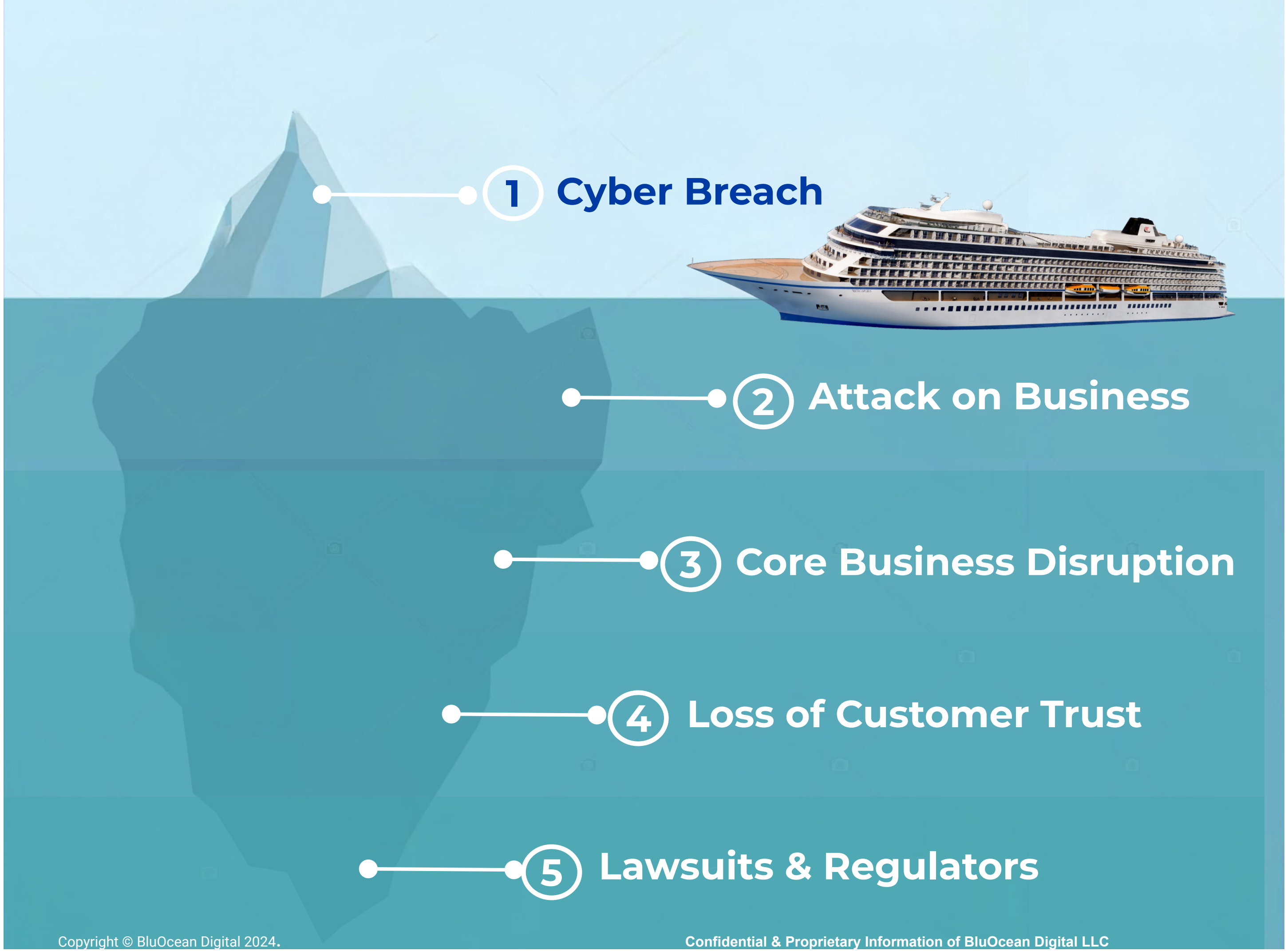
Select period: from Jan 1, 2022 to Dec 31, 2022 Filter

Total Compliance 72%

Unpatched Vulnerabilities 36.2%

Number of New Vulneratbilities 36

Number of Completed Patch Cycles 29



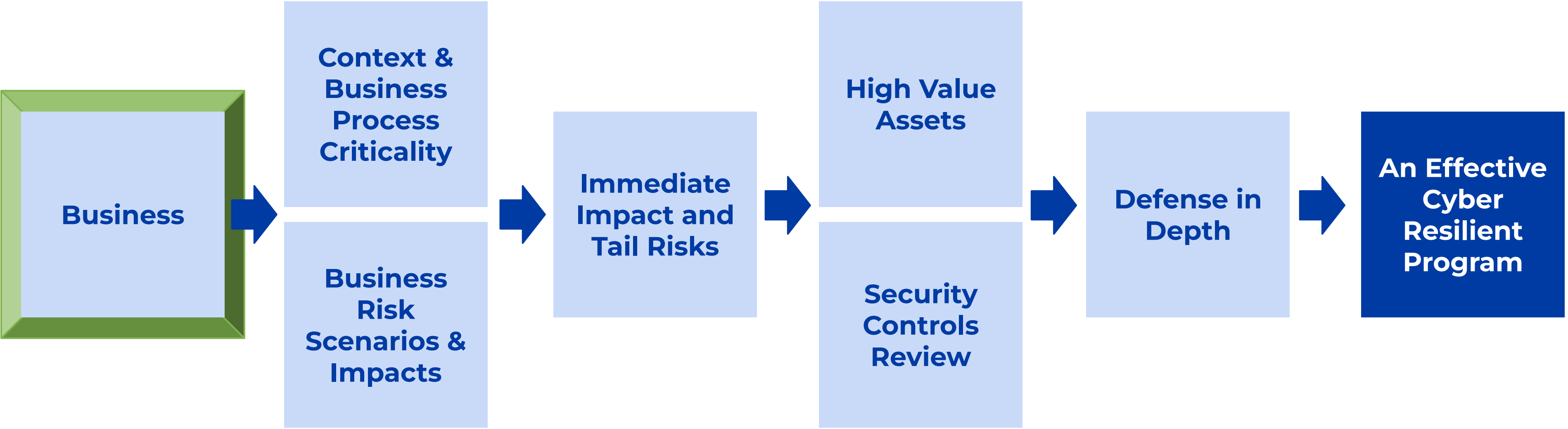
# Reactive

# Vs.

# Proactive

# To enable and protect your business effectively, you need to start by understanding

## “How does the business operate?”


Business
Context & Business Process Criticality
Business Risk Scenarios & Impacts
Immediate Impact and Tail Risks
High Value Assets
Security Controls Review
Defense in Depth
An Effective Cyber Resilient Program

# How do Cyber Criminals Attack a Business?

They enter. Criminals will target common vectors like phishing and malware

They sit quietly and learn. The average breach detection time is 118 days

They make moves for financial gain $$$$

- There was $1.1 billion in ransom paid in 2023. Outside of ransom payments, the average cost of ransomware incident was over $5 million

# Understanding Your Business is the First Step

## If you don’t know how it operates how you protect it?

Start with collaborating with your business leaders and get seat on the strategy table

### CFO

What is our financial exposure if there is a cyber attack?

### Chief Risk Officer

What is our organization’s risk tolerance?

### Business Unit Leads

What business processes are critical for our growth and customers?

### Legal & Compliance

What are our regulatory and contractual obligations?

# Understand what a disruption will look like immediately and in long-term tail risk

## Financial Impact

- Drop in Stock Prices
- Loss of Revenue
- Recovery Costs

## Operational Impact

- Diminished business function
- High costs of manual workarounds

## Regulatory Impact

- Regulatory Fines
- Class Action Lawsuits
- Increased Future Audits

## Reputational Impact

- Loss of customer & investor trust
- Continued diminished financial performance

# Understanding the Weight of Tail Risk: Crowdstrike

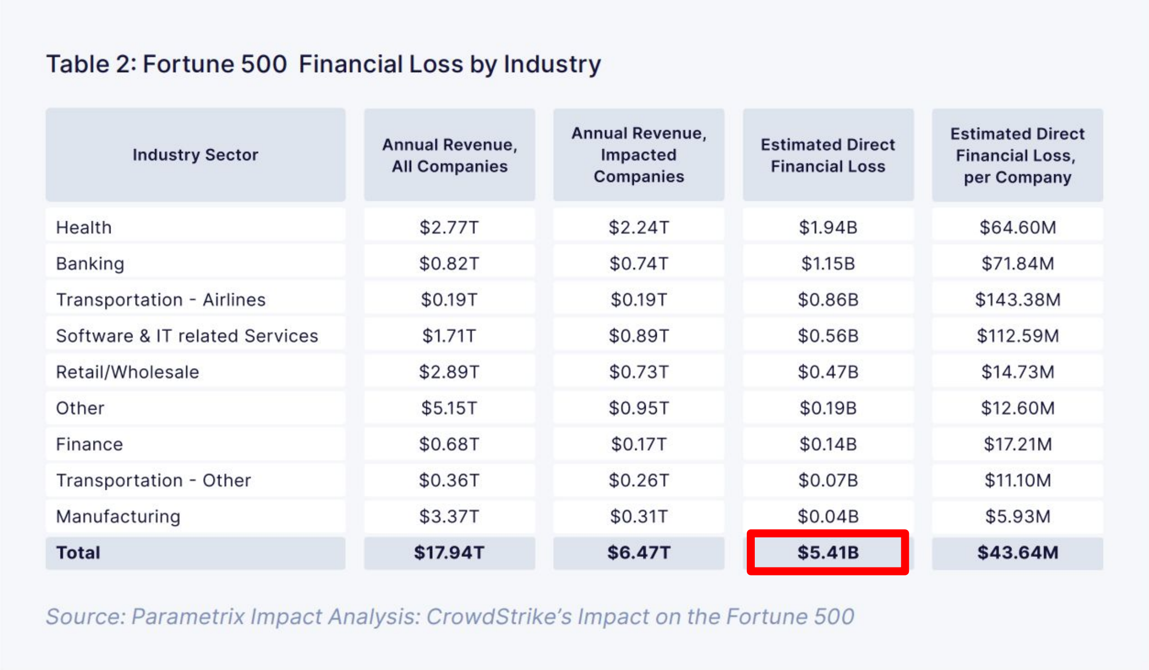


Table 2: Fortune 500  Financial Loss by Industry

| Industry Sector | Annual Revenue, All Companies | Annual Revenue, Impacted Companies | Estimated Direct Financial Loss | Estimated Direct Financial Loss, per Company |
|---|---|---|---|---|
| Health | $2.77T | $2.24T | $1.94B | $64.60M |
| Banking | $0.82T | $0.74T | $1.15B | $71.84M |
| Transportation - Airlines | $0.19T | $0.19T | $0.86B | $143.38M |
| Software & IT related Services | $1.71T | $0.89T | $0.56B | $112.59M |
| Retail/Wholesale | $2.89T | $0.73T | $0.47B | $14.73M |
| Other | $5.15T | $0.95T | $0.19B | $12.60M |
| Finance | $0.68T | $0.17T | $0.14B | $17.21M |
| Transportation - Other | $0.36T | $0.26T | $0.07B | $11.10M |
| Manufacturing | $3.37T | $0.31T | $0.04B | $5.93M |
| **Total** | **$17.94T** | **$6.47T** | **$5.41B** | **$43.64M** |

*Source: Parametrix Impact Analysis: CrowdStrike's Impact on the Fortune 500*

**Estimated that the top 500 US companies by had faced nearly $5.4bn losses, with only $540M - $1.08B insured**

**Delta claims $500M+ loss for over 7000 cancelled flights in a lawsuit**

**5000+ flights across airlines cancelled within the day**

**Stock went down initially ~40% and ~35% a month after incident**

# You have to understand what can go wrong for your business during an attack

# Manufacturing and Supply Chain Scenarios

CLOROX™

SIMPSON Manufacturing COMPANY™

**Example**

Unable to process or fulfill customer orders from your warehouses for 3 weeks due to a ransomware attack.

Impact: **$700M**

# Healthcare Scenarios

**Example**

Unable to admit any patients in to emergency rooms because admissions systems are down.

Impact: **Class Action Lawsuits**

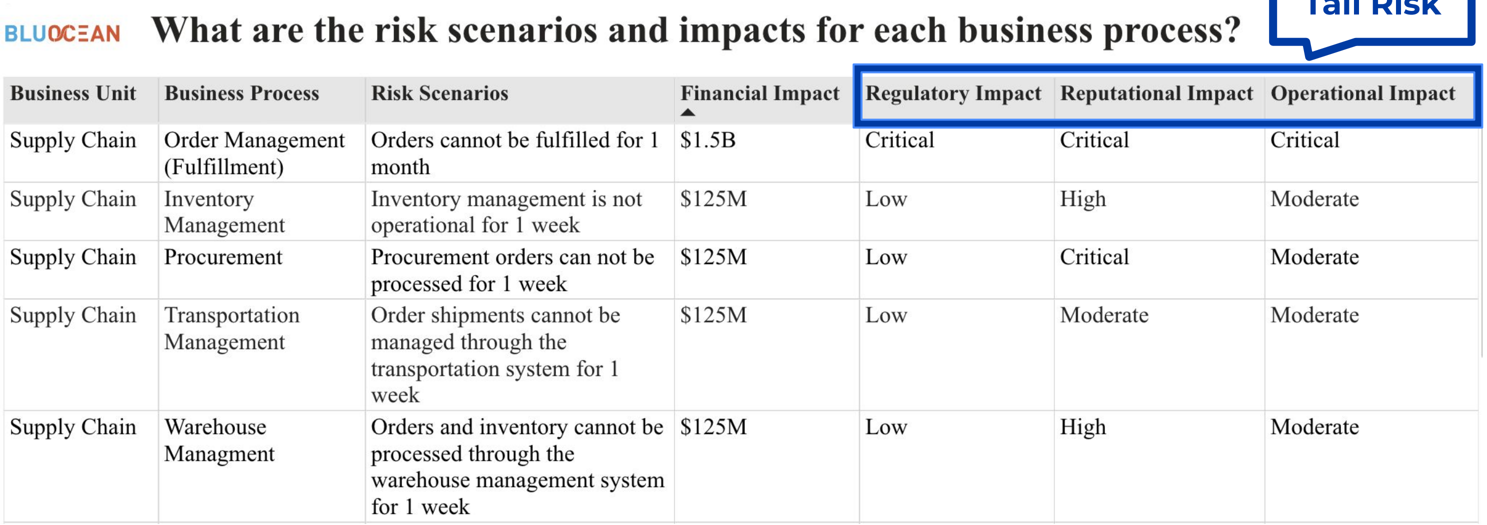
# Financial Services Scenarios

**Example**

Attackers gain control of your customer banking portal and customers cannot securely access their accounts.

Impact: **Regulatory Fines**

# Case Study: Risk Scenarios and Impact



BLUOCEAN **What are the risk scenarios and impacts for each business process?**

| Business Unit | Business Process | Risk Scenarios | Financial Impact ▲ | Regulatory Impact | Reputational Impact | Operational Impact |
|---|---|---|---|---|---|---|
| Supply Chain | Order Management (Fulfillment) | Orders cannot be fulfilled for 1 month | $1.5B | Critical | Critical | Critical |
| Supply Chain | Inventory Management | Inventory management is not operational for 1 week | $125M | Low | High | Moderate |
| Supply Chain | Procurement | Procurement orders can not be processed for 1 week | $125M | Low | Critical | Moderate |
| Supply Chain | Transportation Management | Order shipments cannot be managed through the transportation system for 1 week | $125M | Low | Moderate | Moderate |
| Supply Chain | Warehouse Managment | Orders and inventory cannot be processed through the warehouse management system for 1 week | $125M | Low | High | Moderate |

**Tail Risk**

**Each scenario was assessed for potential financial impact and tail risk impact, with insights validated through finance and ERM.**

**This assessment is leveraged to pinpoint processes with the highest risk exposure.**

# Attacks on High Value Systems supporting mission critical processes

**Attackers are still targeting crown jewels but in a new way**

**Ticketmaster had a ransom request of $440K for 560M records, fractions of a penny per record!**

**Crown jewels are now critical business process**

**Banks - Customer Applications**
**Manufacturing - Order Management Systems**
**Healthcare - Electronic Health Record Systems**

# How Vulnerable Are Your Critical Assets?

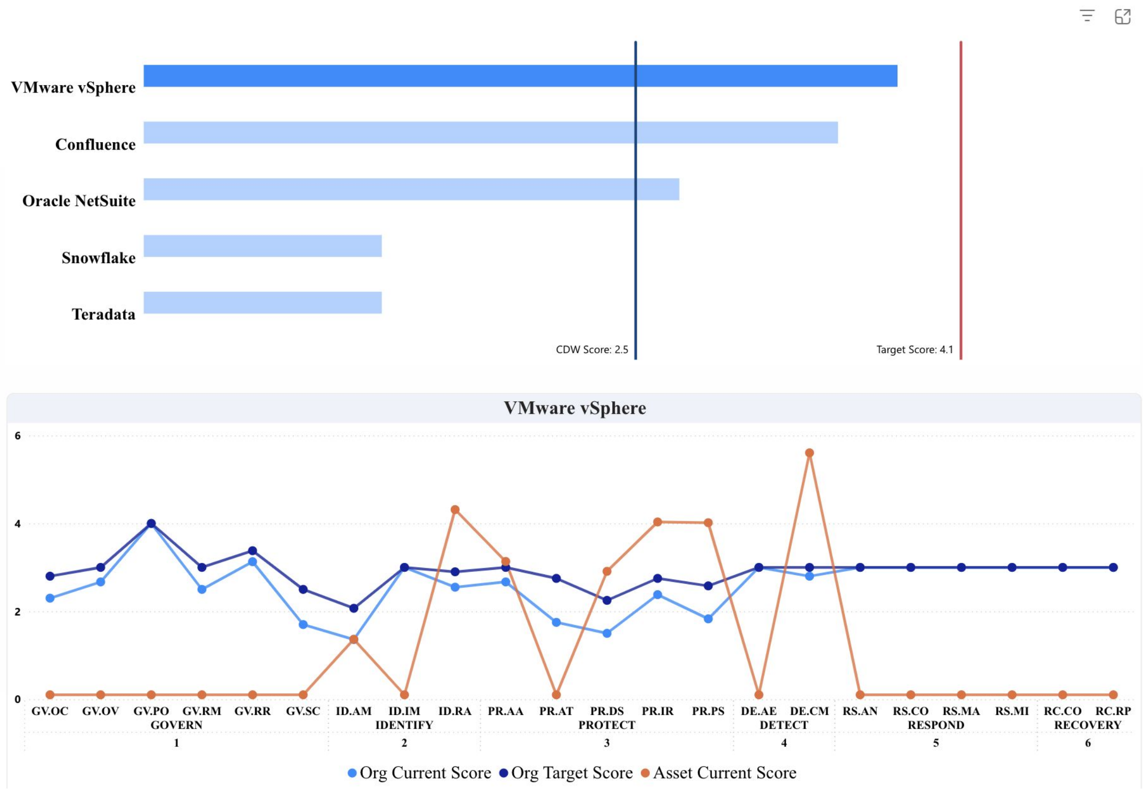
Determined hackers will likely penetrate your perimeter controls through phishing or other means

Your Job is to "Make it difficult for them to attack high value assets through layered defense"

Build an asset centric view for your crown jewels that support critical business processes

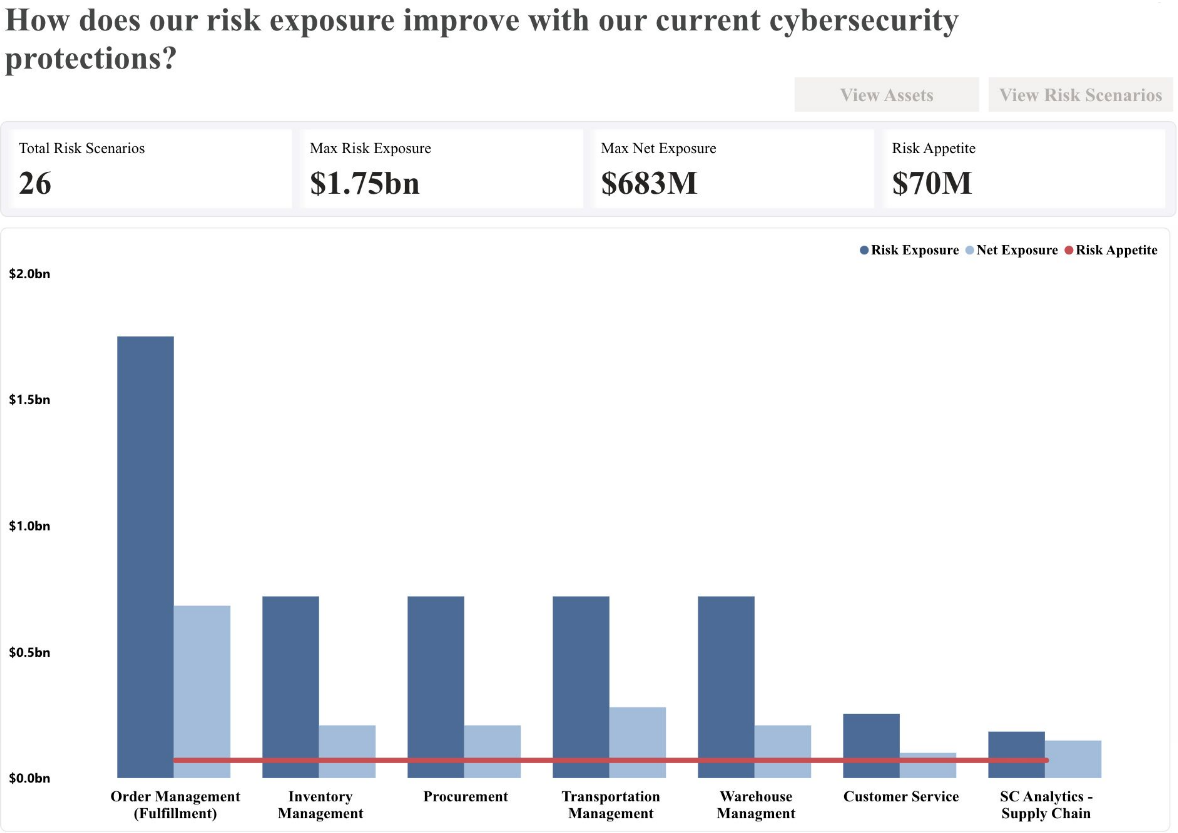
# Case Study: Critical Asset Protections

How do asset maturity scores compare to target based on our risk appetite?



**The analysis focuses on evaluating strength of cybersecurity controls for high value assets associated with critical business processes.**

# Case Study: Understanding the Effectiveness of Current Cyber Program



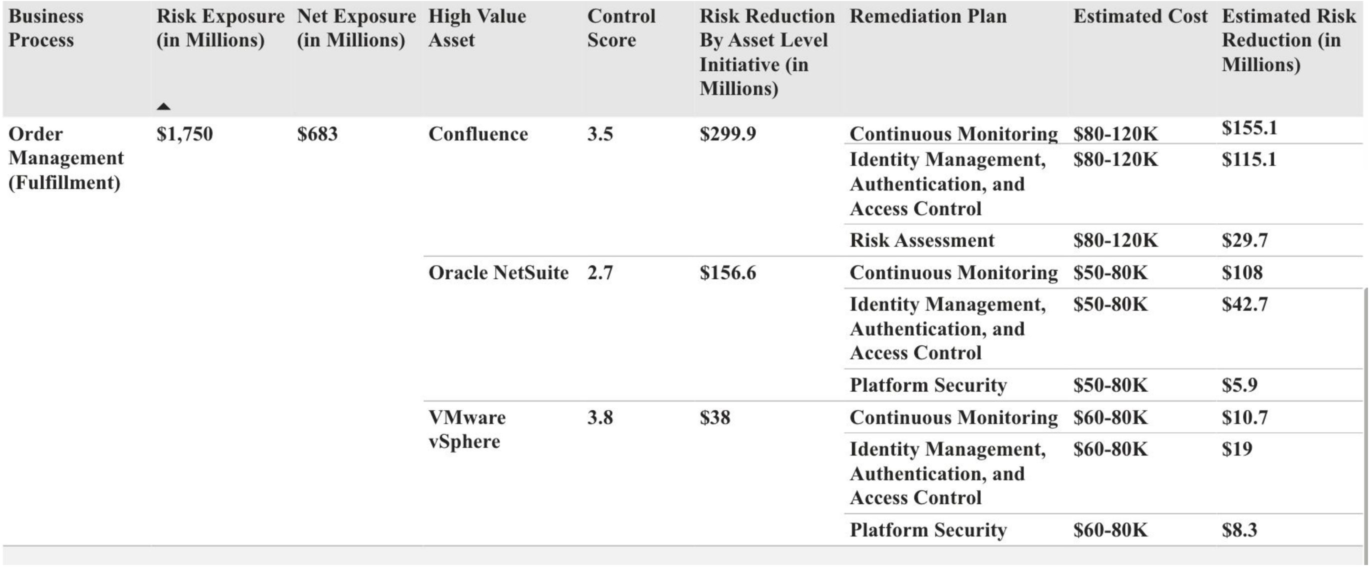
**How does our risk exposure improve with our current cybersecurity protections?**

| Total Risk Scenarios | Max Risk Exposure | Max Net Exposure | Risk Appetite |
|---|---|---|---|
| 26 | $1.75bn | $683M | $70M |

**Evaluating whether current strength of cybersecurity controls is sufficient to reduce critical process risks to acceptable levels (Risk Appetite)**

**Business and the Security team can leverage this analysis to identify the processes and associated assets that need to be remediated on priority**

# Case Study: Planning Driven By Business Risk Reduction



| Business Process | Risk Exposure (in Millions) | Net Exposure (in Millions) | High Value Asset | Control Score | Risk Reduction By Asset Level Initiative (in Millions) | Remediation Plan | Estimated Cost | Estimated Risk Reduction (in Millions) |
|---|---|---|---|---|---|---|---|---|
| Order Management (Fulfillment) | $1,750 | $683 | Confluence | 3.5 | $299.9 | Continuous Monitoring | $80-120K | $155.1 |
| | | | | | | Identity Management, Authentication, and Access Control | $80-120K | $115.1 |
| | | | | | | Risk Assessment | $80-120K | $29.7 |
| | | | Oracle NetSuite | 2.7 | $156.6 | Continuous Monitoring | $50-80K | $108 |
| | | | | | | Identity Management, Authentication, and Access Control | $50-80K | $42.7 |
| | | | | | | Platform Security | $50-80K | $5.9 |
| | | | VMware vSphere | 3.8 | $38 | Continuous Monitoring | $60-80K | $10.7 |
| | | | | | | Identity Management, Authentication, and Access Control | $60-80K | $19 |
| | | | | | | Platform Security | $60-80K | $8.3 |

Identify controls that need to be implemented to bring net risk below risk appetite.

Remediation initiatives enable CISO to answer:

- Which security investments reduce the most risk?
- What is the estimated cost across each high value asset?

# With this new understanding of effectiveness, you are now ready to….

Proactively approach protecting your business from a cyber attack

Ensure cyber investments protect key business priorities

Continuously monitor risk to core business priorities

# Regulators now also expect you to assess your cyber program's effectiveness in protecting your business

***Material Incident Reporting***

***Risk Management Strategy***

***Governance***

**You need to know which processes, if attacked, impact will become material to your business!**

**Reduce material cyber risks to the business**

**Board and Management are on the hook! They need to be engaged - Not just informed**

# How a Business Centric Cyber Program Builds a Foundation for SEC Rule

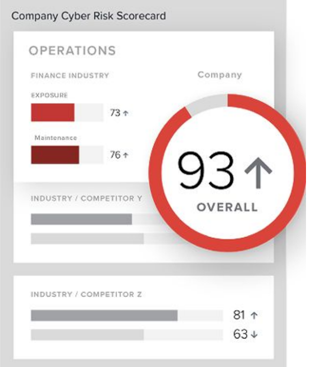
Engages business leaders to ***identify the cyber risks*** they care about

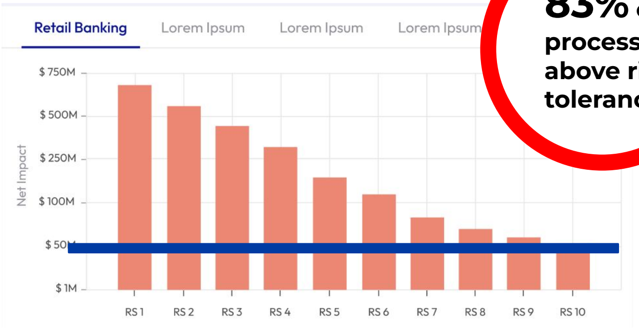
**Works across business units** to build a model quantifying materiality for cyber risks that impact high value assets

**Uses the business to prioritize cyber risks,** factoring in projected growth and technology automation

**CISOs and business leaders** collaborate to **align security initiatives** with **identified business risk**

# The Road Forward: Effectiveness is the new Cybersecurity Benchmark!





**83%** of processes above risk tolerance

Gaps in framework → Gaps in protection of mission critical business process

Comparison to peers → Comparison to enterprise risk tolerance

Inform board on improvements in cyber program posture → Engaged board because it's about EFFECTIVENESS in reducing risks to the business strategy

# Takeaways

## *Think like a cyber criminal to build an "effective" Cyber Program!*

1. Know what your business cares about
2. Understand how it operates
3. Conduct risk scenario analysis (how would a criminal exploit you!)
4. Identify the associated assets and interdependencies
5. Build and implement layered defense for each asset
6. Ensure cyber investments protect key business priorities & assets
7. Proactively monitor risk to core business processes

# Thank You!

## Contact Me

## Sign Up for Our Newsletter