BLOOMINGTON - NORMAL
INNOVATION
ALLIANCE

Walt Powell
Lead Field CISO
*Global Security Strategy Office - **CDW***

CYBER SECURITY AS AN INVESTMENT THESIS

BOTTOM LINE UP FRONT (BLUF)

- In the news daily, **Cyber Threats** continue to be one of the key challenges for organizations.
- **Cyber Security is becoming "mission critical"** for every organization.
- **The "cost"** of not investing in security and risk management **is more than just the fines and penalties that come after a data breach**
- You can **control the costs by understanding your risk exposure** and how that compares to your risk appetite.
- Once you understand your exposure you can **transfer or buy-down risk** to meet your operational goals.
- Security is more than risk reduction, **Cyber Security can make the businesses scalable, resilient, and appealing to customers.**

$5 MILLION

AVERAGE COST OF A DATA BREACH IN 2023

24 DAYS

AVERAGE AMOUNT OF PRODUCTION DOWNTIME FOR RANSOMWARE VICTIMS IN 2022

SHOW OF HANDS

WHO'S ORGANIZATION IS TOO SMALL, OR INFORMATION IS NOT VALUABLE ENOUGH TO BE A TARGET?

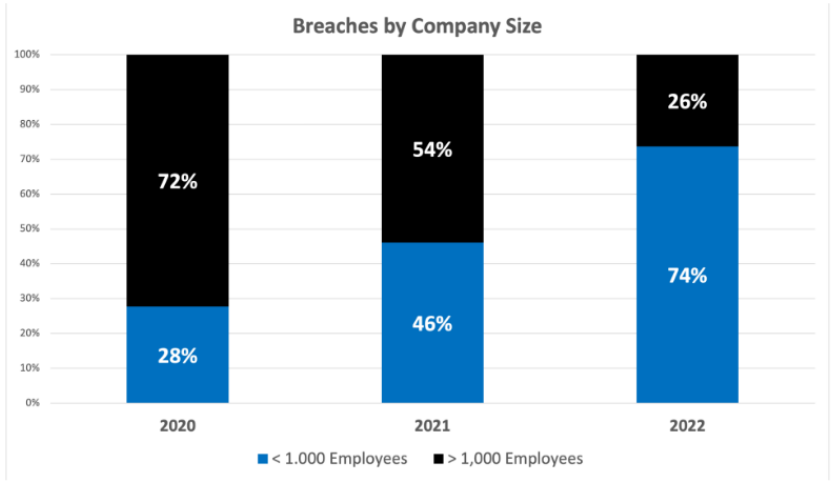
BLOOMINGTON - NORMAL INNOVATION ALLIANCE

THE MIDMARKET IS OVER-REPRESENTED

CYBERSECURITY

Mid-Sized Businesses are Overrepresented

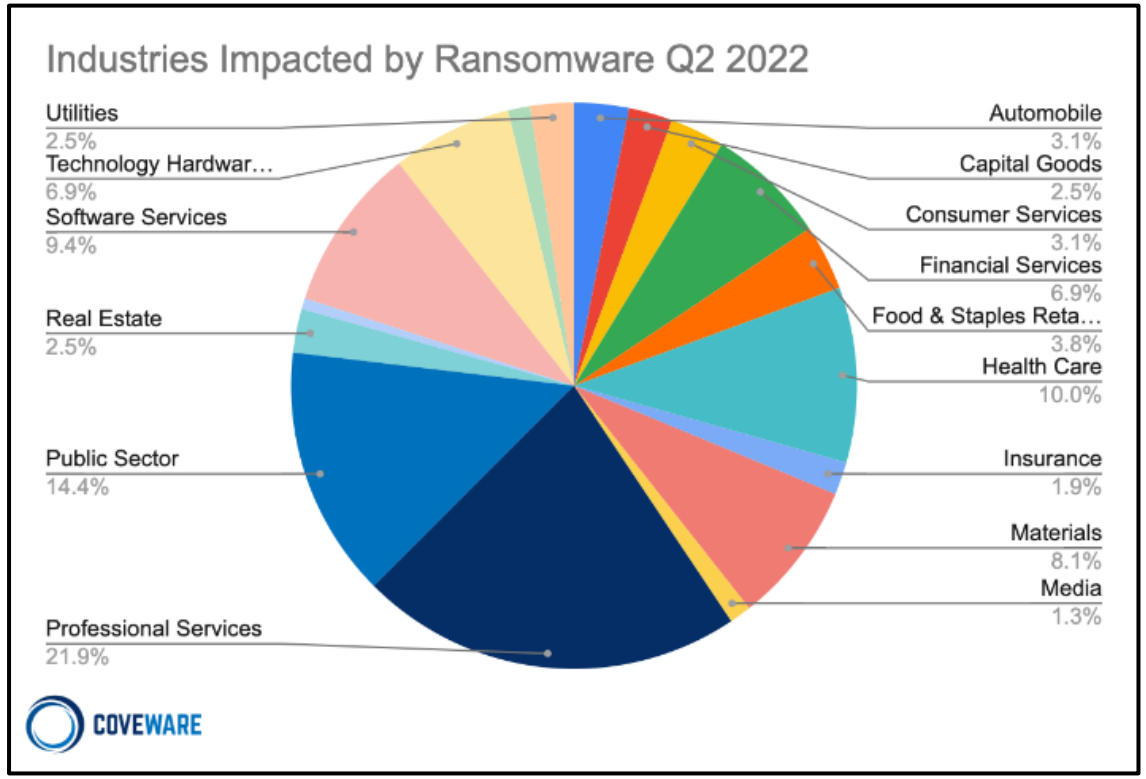
Organizations with fewer than 1000 employees experienced over **2/3 more breaches** than those with greater than 1000.



Graph based on data from
Verizon 2023 Data Breach Investigations Report

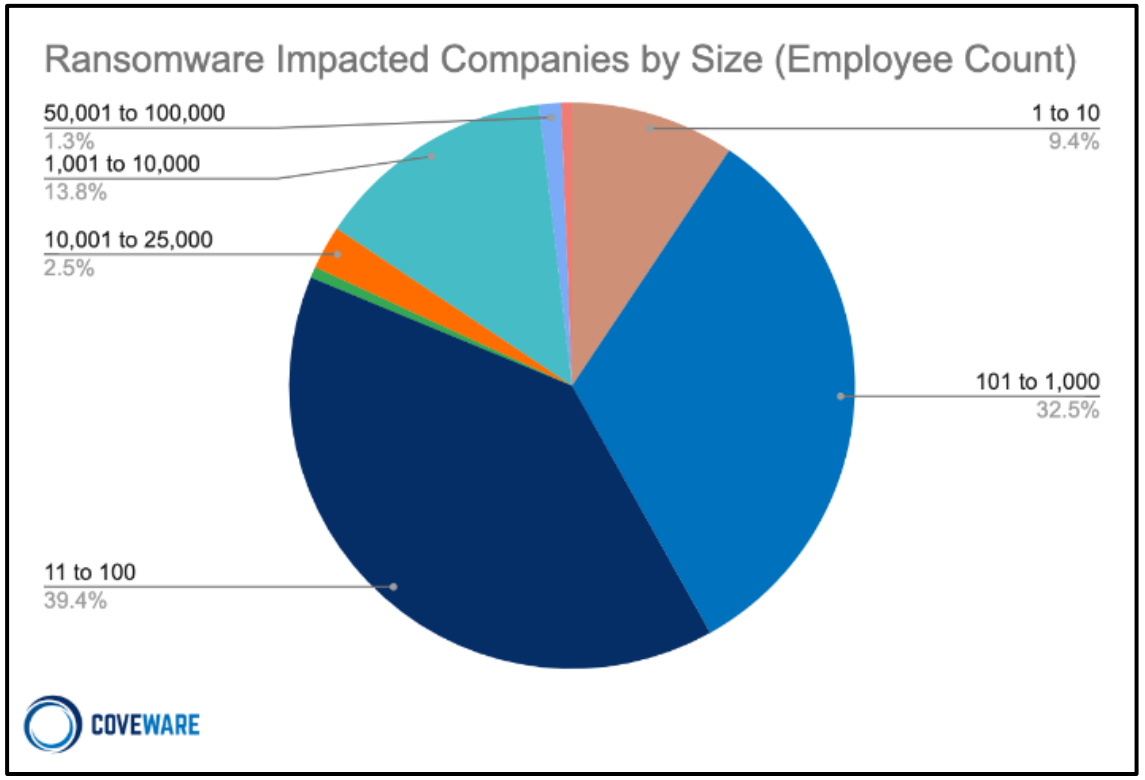
Verizon DBIR via NextDLP

EXTORTION TARGETS



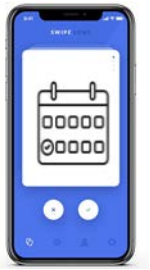
All industries are targets

SMBs get attacked the most



Coveware Q4 2021 Ransomware Report

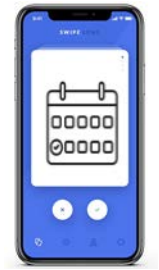
DIGITAL TRANSFORMATION



JOE’S CORNER TIRE

TECHNOLOGY IS THE WHOLE BUSINESS

ADVERTISING,
SEO, REVIEWS
SOCIAL MEDIA



APPOINTMENT
BOOKING
MOBILE APP

POINT OF SALE,
PAYMENT CARD,
LOYALTY/ REWARDS

ACCOUNTING,
PAYROLL, HR, CRM
SAAS

ORDERING, INV
MGMT, -WEB APP

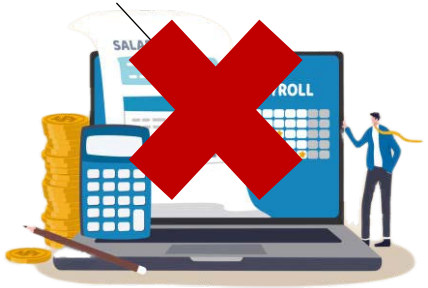
JOE'S CORNER TIRE

CYBER SECURITY IS THE WHOLE BUSINESS

DATA BREACH

POINT OF SALE, PAYMENT CARD, LOYALTY/ REWARDS

BUSINESS EMAIL COMPROMISE (BEC)

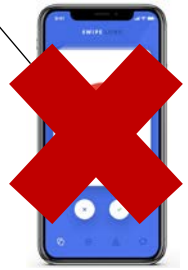


ACCOUNTING, PAYROLL, HR, CRM SAAS

DDOS

APPOINTMENT BOOKING MOBILE APP

REVIEW BOMBING



ADVERTISING, SEO, REVIEWS SOCIAL MEDIA

JOE'S CORNER TIRE

SUPPLY CHAIN OR API ATTACKS

ORDERING, INV MGMT, -WEB APP

MISSION CRITICAL

Legal Precedence

Caremark International, Inc. Case

Court held that **failure** of a corporate director to make a **good faith attempt at insti[illegible] effe[illegible] compliance program** may in some situations constitute a **breach of a director's duc[illegible] du[illegible]** and directors **could be held personally liable**

Marchand (Blue Bell Ice Cream) v. Barnhill

Court held that failure to implement a **"reasonable"** system of monitoring and reporting for essential and 'mission critical' activities and could constitute a **breach of duty of loyalty**

The Boeing Co. Case

Court extended the definition and scope of **'mission critical"** activities to include large corporations and not just monoline product companies.

McDonald's Corp. Case

Court extended the **fiduciary duty** from just directors to include Officers. Critical parts of an officer's job are "**to identify red flags, report upward, and address them if they fall within the officer's area of responsibility**," and (ii) "**to gather information and provide timely reports to the board about the officer's area of responsibility.**"

Proposed SEC Cyber Rules

Overview of SEC Cyber Rules

The SEC recently proposed new rules that would require public companies to disclose material cyber security incidents to the SEC more quickly and to provide more detailed information about those incidents. The rules would also require public companies to implement a number of cyber security measures, such as having a board-approved cyber security program and conducting regular cyber security assessments.

SEC Enforcement Actions

The SEC has taken a number of enforcement actions against companies that have failed to implement adequate cyber security programs. For example, in 2018, the SEC fined Equifax $175 million for failing to protect the personal information of millions of consumers. In 2019, the SEC fined Marriott International $20 million for failing to protect the personal information of millions of hotel guests.

These rules are not yet accepted as of June 2023 the have been indefinitely delayed and sent back to comment period.

FTC CONSENT ORDERS

2019 FTC Consent Order

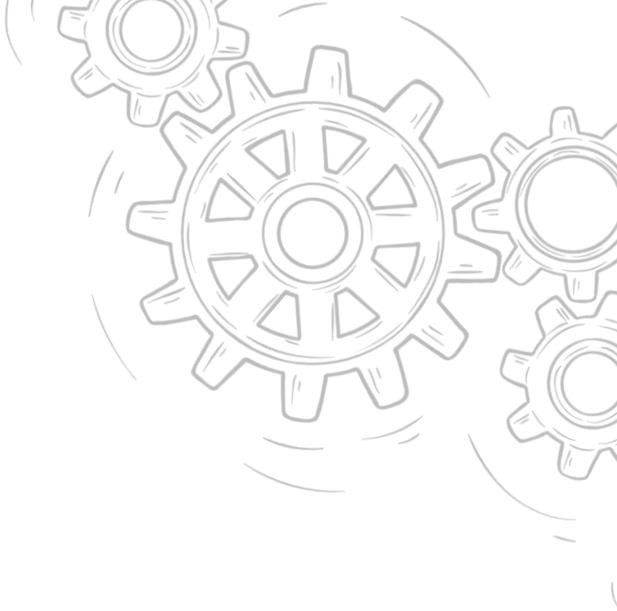
2009 FTC Consent Order

Provisions

I. Mandated Information Security Program

IT IS FURTHER ORDERED that each Covered Business shall not transfer, sell, share, collect, maintain, or store Personal Information unless it establishes and implements, and thereafter maintains, a comprehensive information security program ("Information Security Program") that protects the security, confidentiality, and integrity of such Personal Information. To satisfy this requirement, each Covered Business must, at a minimum:

IT IS FURTHER ORDERED that respondent, and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, limited liability company, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:



CYBER SECURITY AS A BUSINESS DRIVER

BLOOMINGTON - NORMAL
INNOVATION
ALLIANCE

WHAT PROVIDES VALUE TO YOUR ORGANIZATION?

- **Who determines Value?**
  - Stockholders
  - Partners
  - Owners
  - VC / PE Firms
  - Hedge Funds
- **What Delivers value?**
  - Share price
  - Dividends
  - Capital Appreciation
- **Where is value created?**
  - Assets
  - Market-based
  - Discounted Cash Flow
- **When is value created?**
  - Quarterly / Annual Dividends
  - Sale of Equity

WHAT PROVIDES VALUE TO YOUR ORGANIZATION?

How is value determined?

- Stock price
- Revenue growth (CAGR)
- EBITDA
- Cash flow
- Price-to-earnings ratio (P/E ratio)
- Profit margins
- Earnings per share (EPS)
- Customer acquisition cost (CAC)
- Debt-to-equity ratio
- Dividend yield
- Discounted Cash Flow (DCF)
- Customer satisfaction
- Employee satisfaction
- Brand equity
- Market share
- Customer lifetime value (LTV) ratios
- Intellectual property and patents
- Product differentiation and competitive advantage
- Scalability and growth potential
- Exit potential, such as IPO or acquisition opportunities.

Do you know your company's financial targets?

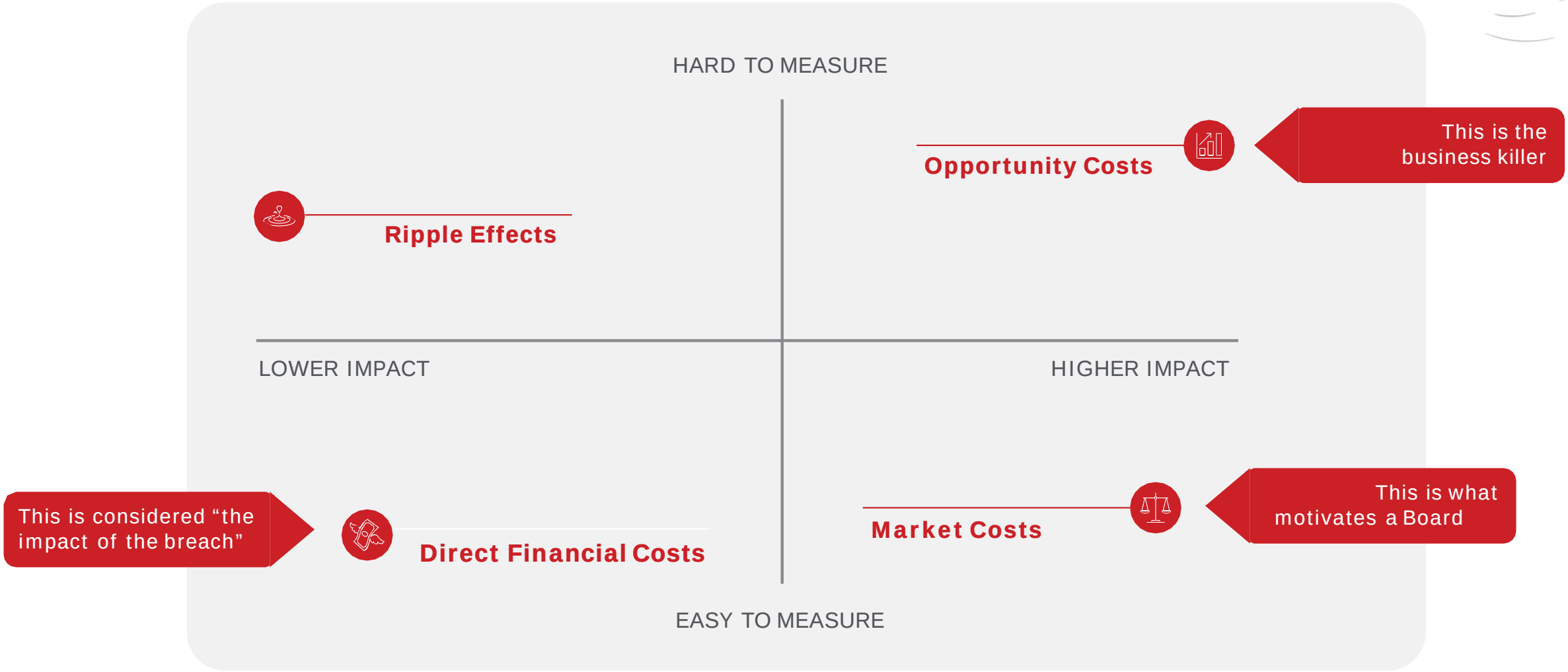
BLOOMINGTON - NORMAL INNOVATION ALLIANCE

RISK IN A BUSINESS CONTEXT

- **Financial**
  - Response Costs
- **Operational**
  - Productivity Loss
- **Regulatory Compliance**
  - Restrictions
  - Fines
- **Legal**
  - Judgements
- **Reputational**
  - Stock Value
  - Customer Churn
- **Strategic**
  - Loss of Competitive Advantage
- **Health & Safety**
  - Loss Of Life

BLOOMINGTON - NORMAL INNOVATION ALLIANCE

THINKING ABOUT THE IMPACTS



TRANSLATING SECURITY INTO THE LANGUAGE OF BUSINESS

Business Justified: Every operational or technical security element can be justified by reference to a risk-prioritized business requirement

Source: SABSA Institute

CDW's C3 COMMON CLIENT CHALLENGES

BOD Challenges	Related CISO Challenges
Production Uptime / Business Continuity	• Business Process Continuity & Resilience
Support Innovation	• Digital Transformation • Agility & Mobility
Reduce Financial Risk. Cost Control & Reduction (Macro Economic Factors)	• Cybersecurity Program Budgeting
Cyber Risk Reduction	• Breach Risk Reduction • Security Strategy & Road Mapping • Cyber Risk Measurement and Communication
Compliance Risk Reduction	• IT Security Regulatory Complexity • IT Compliance Risk
Supply Chain Risk Reduction (Global Unrest, Economic Uncertainty)	• Cyber-Supply Chain Risk Reduction
Resource and Talent Limitations	• Security Talent Shortage • Security Stack Sprawl

BLOOMINGTON - NORMAL INNOVATION ALLIANCE

RISK vs. THREAT

Risk

- Potential for **harm or loss** due to exposure.
- Quantified by assessing the **probability and impact**.
- Supports **informed decisions based on cost**.
- Can be mitigated through risk management strategies such as risk **avoidance**, risk **transfer**, risk **reduction**, or risk **acceptance**.

Threat

- Specific events or **actors that could potentially cause harm** or disruption to an organization, its assets, or its operations.
- Intentional or unintentional, external or internal, and can be caused by **human, environmental, or technological factors**.
- Identified through threat intelligence, and **vulnerability assessments**
- Mitigated through **security measures and controls**

BLOOMINGTON • NORMAL
INNOVATION ALLIANCE

What is Cyber Risk?

Risk = Probability x Impact

Probability
(Threat X Vulnerability)

Impact
(Hard Costs X Soft Costs)

Threat
(Frequency of Contact X Probability of Action)

Vulnerability
(Threat Capability X Resistance Strength)

KPIs vs. KRIs

Indicator Metric	What does it measure?	What is its purpose?	Who is the audience?
Key Risk Indicator (KRI)	Quantify risk A snapshot of an organization's current risk posture and risk mitigation techniques	Non-operational and focuses on risk identification Helps organizations understand the risks involved and the likelihood of not having a positive result	Executive Management and the Board
Key Performance Indicator (KPI)	Measure performance (i.e., how effectively something is operating) Measures how well individuals, business units, projects are performing according to their goals	Provide metrics for operational performance	Operations and Middle Management

REAL WORLD EXAMPLE

BLOOMINGTON - NORMAL
INNOVATION
ALLIANCE

IS KRI MONITORING PROGRAM – PILOT PROGRAM

- As a result of the data analysis performed, an updated listing of KRIs is suggested below to be able to present ***measurable*** and ***reportable*** metrics.
- Further KRIs may result from a more detailed analysis of the data collected.

Original KRI Description	Updated KRI Description
# of outgoing emails that contain unprotected highly sensitive data (i.e., passport numbers, credit card numbers)	# of outgoing ***automated*** emails that contain unprotected highly sensitive data (i.e., passport numbers, DOB)
	# of outgoing ***records*** sent via email containing unprotected highly sensitive data (i.e., passport numbers, DOB)
	# of outgoing ***client communications*** sent via email containing unmasked or unprotected credit card number
# of incoming malicious emails (i.e., malware or phishing attempts) that were detected and blocked by Microsoft Office 365	# of incoming malware attempts that ***were not detected*** by Microsoft Office 365
	# of incoming phishing attempts that ***were not blocked*** by Microsoft Office 365

IS KRI MONITORING PROGRAM – PILOT PROGRAM

- As a result of the data analysis performed, an updated listing of KRIs is suggested below to be able to present ***measurable*** and ***reportable*** metrics.
- Further KRIs may result from a more detailed analysis of the data collected.

Updated KPI Description	Business KRI Translation
# of outgoing ***automated*** emails that contain unprotected highly sensitive data (i.e., passport numbers, DOB)	% Variance against target compliance for outgoing emails that contain unprotected highly sensitive data (i.e., passport numbers, credit card numbers) Per Business Unit % Variance against target compliance for outgoing emails that contain unprotected highly sensitive data (i.e., passport numbers, credit card numbers) Target was set to 0, however current is 150K, so reduction target for Q1 was set to -40% Quantified Exposure Reduction # of emails that contain unprotected highly sensitive data (i.e., passport numbers, credit card numbers) multiplied by $160 (the average per record cost of a data breach per the Ponemon Intitute) **Example: at target a 40% reduction of 150k emails = 60,000 emails x $160 = $9.6M Exposure Reduction**
# of outgoing ***records*** sent via email containing unprotected highly sensitive data (i.e., passport numbers, DOB)	
# of outgoing ***client communications*** sent via email containing unmasked or unprotected credit card number	

RISK QUANTIFICATION

Current Risk Exposure

$134M	Expected Next 12 months
$25M	Minimum
$500M	Maximum
53%	CIS Critical 18 Tier 2 Compliance
$50M	Risk Tolerance
$84M	Risk Exposure Exceedance

Projected Risk Exposure

$90M	Projected 2025
$15M	Minimum
$250M	Maximum
75%	CIS Critical 18 Tier 2 Compliance
$50M	Risk Tolerance
14	IT Security Initiatives
$4.5M	Planned Project Costs

Risk Reduction

$44M

Decrease Due Planned Spend

$40M

Residual Exposure Exceedance

BLOOMINGTON - NORMAL INNOVATION ALLIANCE

CYBER SECURITY AS A FINANCIAL DRIVER

Turn cybersecurity expenditures into cost reductions: Identify cost savings ie; sun-setting legacy systems to reduce licensing and maintenance costs while improving the risk posture.

Turn cybersecurity expenditures into cost avoidance: Help the company avoid costs associated with data breaches or cyber-attacks ie;, investing in employee training and awareness programs to reduce the likelihood of phishing attacks.

Invest in cybersecurity to enable new business models: Use security to enable new business models or revenue streams. ie, investments in blockchain technology and smart contracts can create a secure platform for conducting digital transactions, which could enable new business models and generate additional revenue streams.

Turn cybersecurity expenditures into competitive differentiators: Security can help differentiate from competitors by addressing customer concerns ie; a secure or encrypted mobile app with MFA to attract customers who value security and privacy.

Turn cybersecurity expenditures into revenue generation: Leverage cybersecurity capabilities to create new products or services ie; offering managed services, incident response, or penetration testing, to their customers to generate additional revenue streams.

Align cybersecurity spending with business units: Align with the financial goals of each unit ie; a sales team may prioritize secure collaboration tools to close deals faster, while a finance team may prioritize secure payment processing to reduce the risk of fraud.

BLOOMINGTON - NORMAL
INNOVATION
ALLIANCE

WHERE SHOULD WE BE SPENDING MONEY

There are many wise investments you can make to offset the impact of data breaches.

- **Transfer Risk** to Cyber Liability Insurers
- Insurance providers will expect **Multi-Factor Authentication**
- Breaches cost ***$3.05M LESS*** with Security AI and automation deployed, reducing the breach lifecycle by ***74 days.***
- ***XDR solutions*** improved response times by ***10%.***
- Investing in an ***Incident Response*** team resulted in an average ***$2.66M*** in breach cost savings.
- Regularly testing ***IR*** plans results in ***58%*** cost savings.
- The vast majority (80%) of organizations that have **not** deployed **ZTA spend $1M more** to recover from a breach.

Information Security & Risk Management End User Spending by Segment

2020-2021 (Millions of U.S. Dollars)

Market Segment	2020	2021	Growth (%)
Application Security	3,333	3,738	12.2
Cloud Security	595	841	41.2
Data Security	2,981	3,505	17.5
Identity Access Management	12,036	13,917	15.6
Infrastructure Protection	20,462	23,903	16.8
Integrated Risk Management	4,859	5,473	12.6
Network Security Equipment	15,626	17,020	8.9
Other Information Security Software	2,306	2,527	9.6
Security Services	65,070	72,497	11.4
Consumer Security Software	6,507	6,990	7.4
Total	**133,776**	**150,409**	**12.4**

Source: Gartner (May 2021)

BLOOMINGTON - NORMAL INNOVATION ALLIANCE

CONTROLS INVESTMENT PRIORITIZATION

Data Security

Data Access Governance (DAG) - Varonis,
Data Loss Prevention (DLP) - Digital Guardian

$26.4M	Expected 3yr Total Risk Reduction
$8.8M	Expected Total Annual Risk Reduction
$310K	Year 1 Cost
$186K	Recurring Annual Cost
$682K	**3-Year Total Cost**
$442K - 65%	Tools Cost (Capex)
$249K - 35%	Operational Cost (Opex)
$3.1M	Ransomware
$5.7M	Data Breach
	Annual Risk Reduction By Category
377K%	ROI Ratio
$38.70	Risk Reduction Per Dollar Spent

Identity & Access Management (IAM)

Privileged Identity & Access Management (PIM/PAM) – CyberArk,
Multifactor Authentication (MFA) Expansion - Duo

$27.9M	Expected 3yr Total Risk Reduction
$9.3M	Expected Total Annual Risk Reduction
$425K	Year 1 Cost
$201K	Recurring Annual Cost
$827K	**3-Year Total Cost**
$124K - 15%	Tools Cost (Capex)
$703K - 85%	Operational Cost (Opex)
$7.2M	Ransomware
$900K	Data Breach
$1.2M	Misappropriation
	Annual Risk Reduction By Category
327.3K%	ROI Ratio
$33.73	Risk Reduction Per Dollar Spent

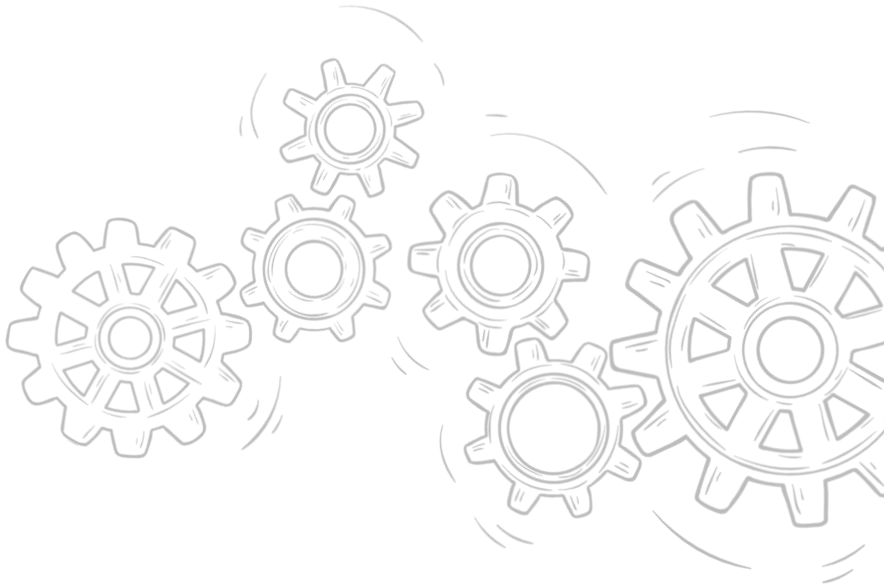
BLOOMINGTON - NORMAL INNOVATION ALLIANCE

KEY TAKEAWAYS

1. The “cost” of not investing in security and risk management is more than just the fines and penalties that come after a data breach
2. In fact, that is often the least important (yet most publicized) cost
3. When talking with Boards and other executives, emphasize the potential market and opportunity costs.
4. Emphasize that Security is *more than risk reduction*. It makes the business scalable, resilient, and appealing to customers
5. **Tell a story** about how security investments are driving forward a holistic strategy, which will continue to amplify benefits and reduce risks over time

QUESTIONS

BLOOMINGTON - NORMAL
INNOVATION
ALLIANCE



THANK YOU

Walt Powell

Lead Field CISO – **CDW**

Walt.Powell@cdw.com

816.204.1253