NOVUS INSIGHT

Technology that empowers.

Hackers, Ransomware, and Data Leaks—Can Your Nonprofit Afford the Risk?

Understanding cyber threats and risk management strategies

Greg Bugbee, CISSP, CISO

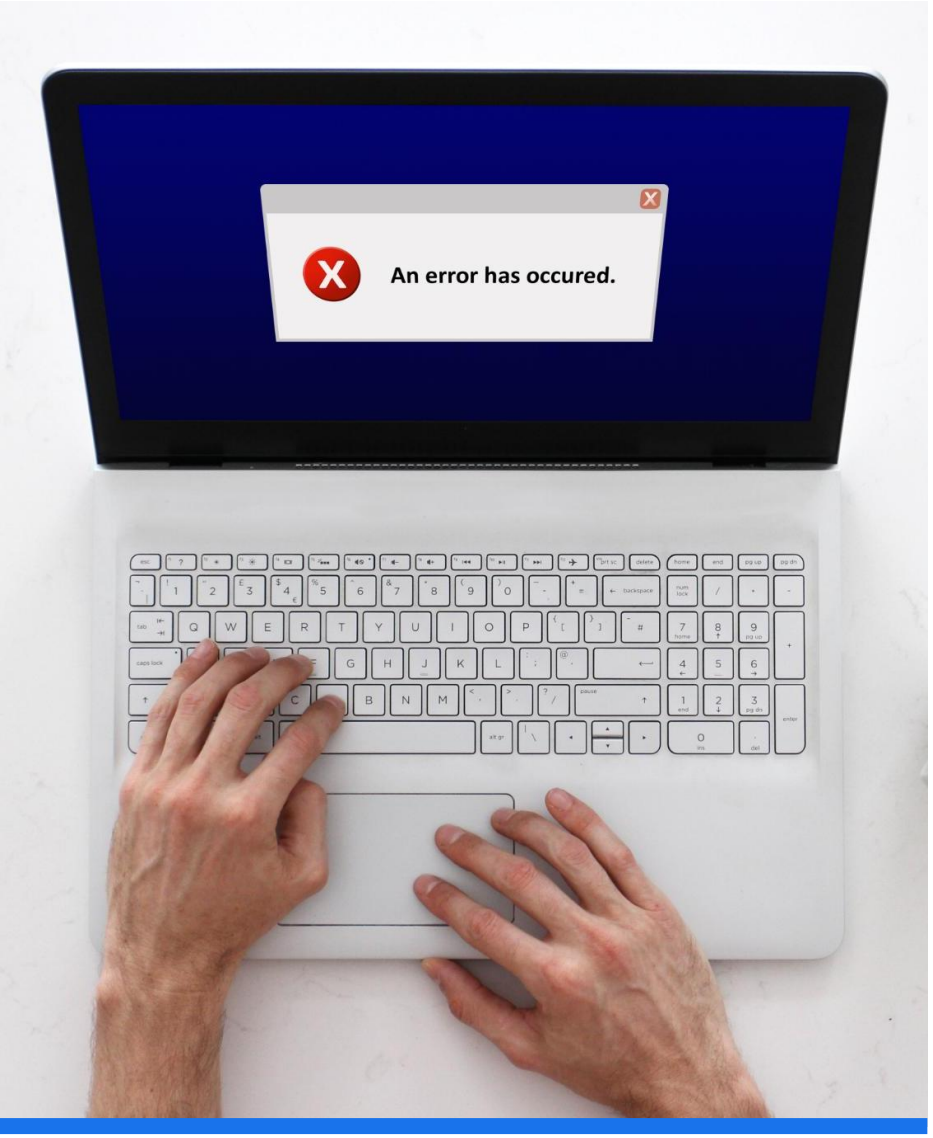
Agenda Items

- Introductions
- The Big Scaries!
- Understanding Cyber Threats Facing Nonprofits
- Financial Impact of a Cyber Incident
- Assessing and Reducing Cyber Risk
- 10:30- Quick break…and Q&A
- Cyber Insurance and Risk Management
- Actionable Strategies for Cyber Protection
- Wrap up and Q&A

Tell us what you think:

- What is the number one catastrophic cyber incident that could happen?
- What is it about the scenario that makes it catastrophic?
- What are you currently doing to protect yourself from this catastrophic thing from happening?

Understanding Cyber Threats Facing Nonprofits



Types of Cyberattacks Targeting Nonprofits

Phishing Attacks

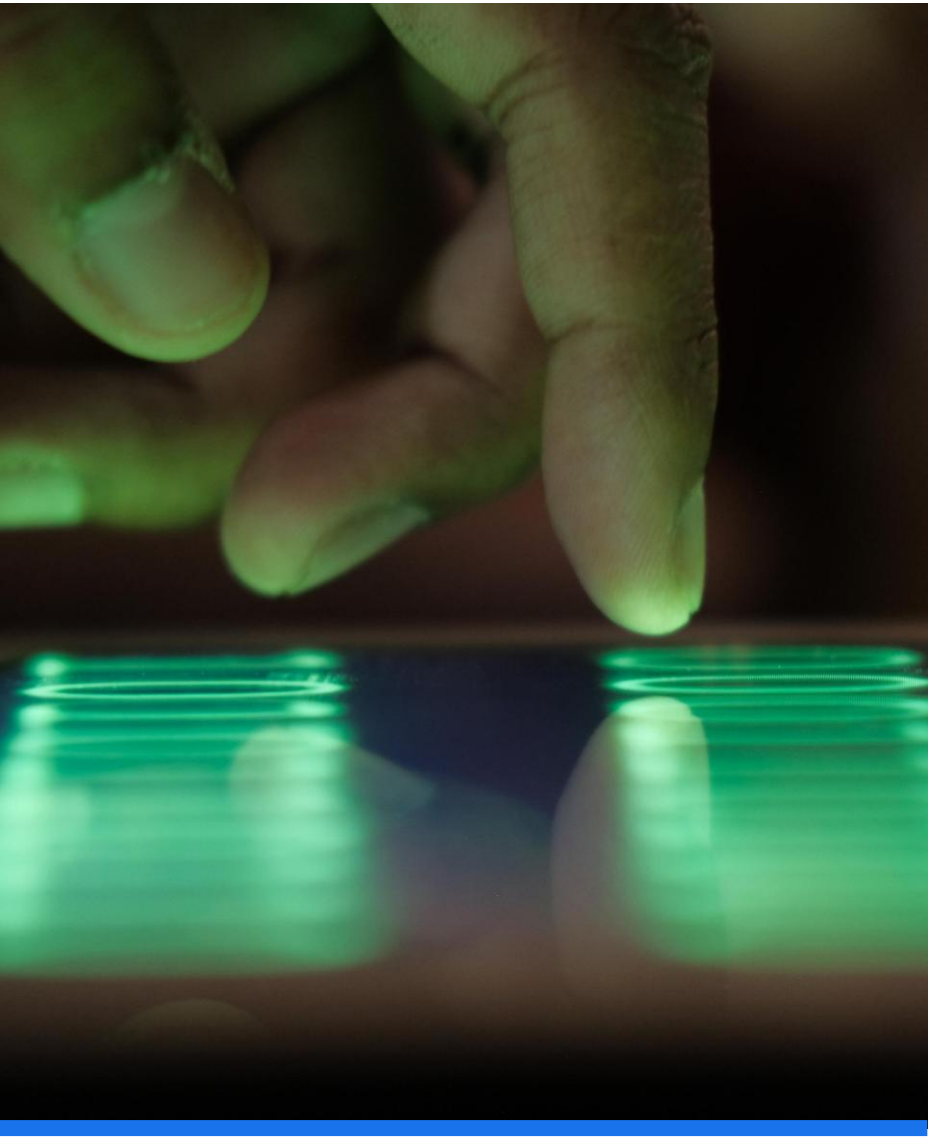
Phishing attacks often target nonprofits through deceptive emails, aiming to steal sensitive information

Ransomware Attacks

Ransomware attacks can lock nonprofit organizations out of their data, demanding payment for restoration of access.

Data Breaches

Data breaches expose sensitive information, leading to data loss and potential legal issues for nonprofits.



Why are nonprofits attacked?

Everyone is a target, and an org isn't too small or not valuable enough to attack- if there's a dollar to steal, someone wants to steal it.

Budget challenges- yeah, there's that pesky overhead thing again. The reality is that you have to protect data or meet certain obligations to run a program, then those costs are direct program expenses.

Valuable data- Medical information, employee data, donor data, and more...

Hacktivism- Nonprofits may be targets due to the causes they represent

Trusted access to others- Nonprofits can provide access to larger targets through their connections- wealthy donors, government organizations, other nonprofits, and funders.

Understanding Phishing Attacks

- Phishing attacks use deceptive emails to trick users.
- Attackers pose as trusted entities to gain information.
- Victims may unknowingly reveal sensitive details, including their credentials.
- Phishing can lead to identity theft and financial loss.
- Awareness, caution, and a good email filter are key to prevention.
- 1 in 3 breaches can be directly traced back to phishing!

Understanding Ransomware Attacks

- Ransomware locks data until a ransom is paid.
- Nonprofits can lose access to critical data.
- Recovery can be costly and time-consuming.
- Ransomware attacks on nonprofits have doubled in the past year.
- In 2024, 58^% of organizations affected by ransomware were compelled to halt operations for recovery.
- 96% of ransomware incidents analyzed in 2024 involved data theft.

Consequences of Data Breaches

- Data breaches expose sensitive donor and client information.
- Legal actions and compliance issues can arise.
- Reputational damage can affect future funding.

Understanding Business Email Compromise

- Business Email Compromise (BEC) targets organizations via email.
- Fraudsters impersonate executives to authorize fund transfers.
- BEC schemes often exploit social engineering tactics.
- Financial losses from BEC can be significant.
- Preventive measures include employee training and verification protocols.
- Examples-
  - Save the Children- $1 million loss
  - San Francisco non-profit- $650,000

Game Break! Identify the Threat: Cybersecurity Challenge

- Analyze various cyber threat scenarios
- Evaluate potential vulnerabilities and identify threats in each scenario.
- Discuss preventive measures to mitigate identified risks effectively.

Financial Impact of a Cyber Incident

Cost Breakdown: Response and Recovery

Forensic Investigations

Forensic investigations are crucial for understanding the impact of a cyber incident, often leading to significant expenses.

Legal Fees

Legal fees can quickly accumulate due to the need for compliance with regulations and potential litigation following a cyber incident.

System Restorations

Restoring affected systems is a critical step in response and recovery, often incurring substantial costs for repairs and updates.

Reputational Damage and Loss of Donor Trust

Impact of Cyber Incidents

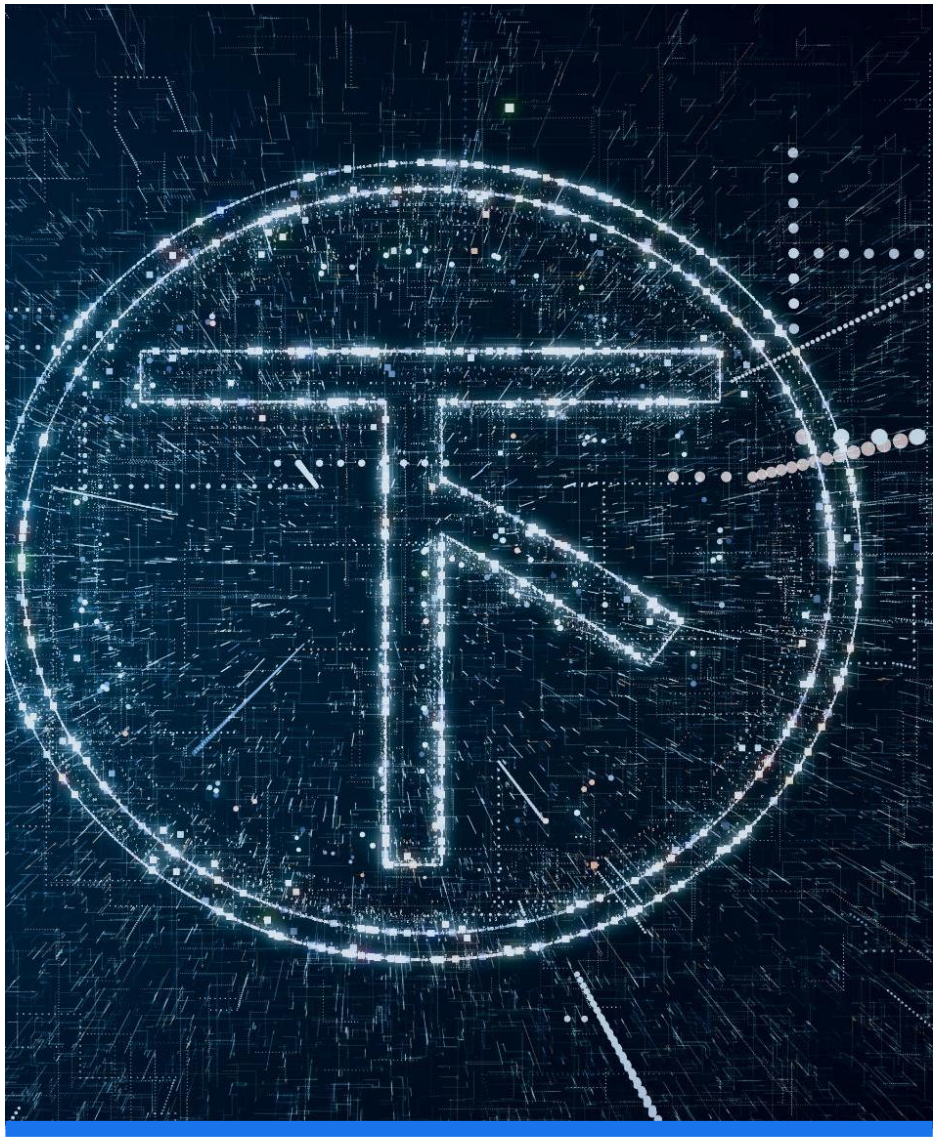
Cyber incidents can severely damage an organization's reputation, leading to a decline in donor confidence and support.

Loss of Donor Trust

When trust is compromised, donors may withdraw their support, making fundraising efforts increasingly difficult.

Long-term Effects

The repercussions of reputational damage can last for years, affecting organizational credibility and future fundraising initiatives.



Interactive Simulation: Financial Threat Exercise

Cyber Incident Simulation

The simulation allows participants to experience the financial impact of a cyber incident in real-time, enhancing their understanding of potential risks.

Understanding Financial Risks

Participants will learn to identify and assess the financial implications of cyber threats through engaging scenarios that simulate real-world challenges.

Importance of Preparedness

This exercise emphasizes the need for preparedness against cyber incidents, reinforcing strategies to mitigate financial losses.

The 'Record' of Doom!

- A record is like a digital fingerprint, except less cool.
- It's what hackers dream of – personal data on a platter!
- In cyber terms, a record is anything that can be stolen and shared
- Records have value to attackers and can be bought and sold

Identifying Your Organization's Records

- What types of records does your organization maintain?
  - Employees
  - Donors
  - People you serve
- How many records do you have?
- Where are they?
- Who has access to them?

Data Hoarding: Risks and Solutions

- **Clutter:** Just like a hoarder's house, your data storage can become cluttered and hard to navigate.
- **Security Risks:** Old records can be a goldmine for cybercriminals.
- **Increased Costs:** Storing unnecessary data can be expensive.
- **Compliance Issues:** Keeping data longer than necessary can lead to legal troubles.

Solution: Data Retention Program

If you don't have the data, the attackers won't either!

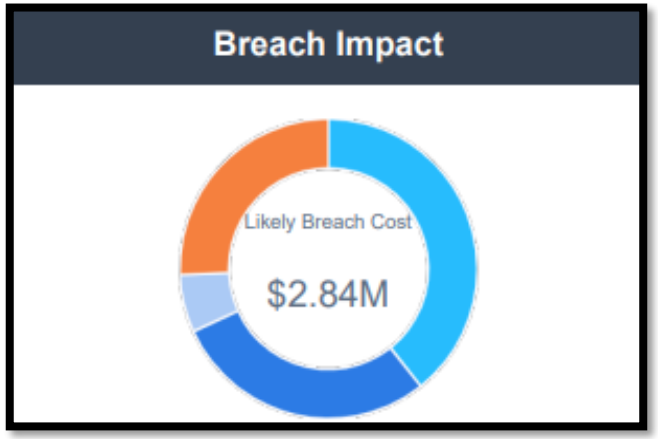
If you do have excess data and it is stolen, it could be a very expensive process to deal with it.

Risk Scenario: Ransomware Attack

Scenario:
Malicious software encrypts a nonprofits' systems, halting operations and demanding payment for recovery.

Primary Impacts:

- **Operational Disruption** (immediate halt to services)
- **Financial** (ransom payment, recovery costs, fines)
- **Loss of Productivity** (days to weeks of downtime)
- **Reputational** (visible service outages)
- **Legal/Compliance** (if data is also exfiltrated)



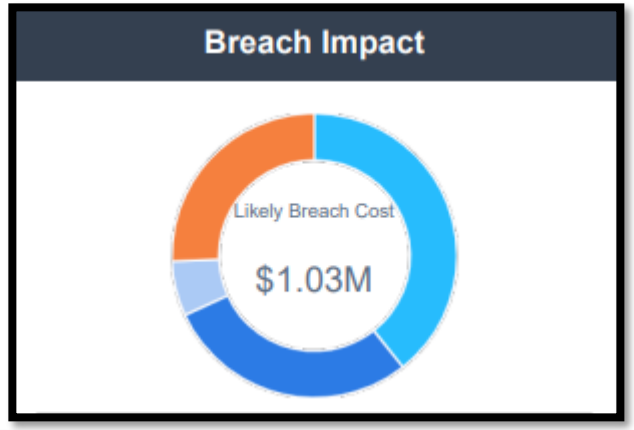
Industry	Breach Type
Public	Ransomware
Est. Industry Breach Cost	**Est. Data Lost**
$2,842,430.09	16,927 records

Risk Scenario: Breach of Personally Identifiable Information (PII)

Scenario:
Unauthorized access to client or employee data leads to a data breach of sensitive personal information.

Primary Impacts:

- Legal/Compliance (breach notifications, regulatory response)
- Financial (credit monitoring, breach notification, regulatory fines)
- Reputational (loss of public trust, media coverage)
- Identity Theft Risk (impact to clients or staff)
- Long-Term Fallout (oversight investigations, strained donor and client confidence)



Industry	Breach Type
Public	PII Breach

Est. Industry Breach Cost	Est. Data Lost
$1,030,643.52	1,991 records

Assessing and Reducing Cyber Risk

Risk Management: An Overview

Risk management is the process by which organizations (1) **identify** potential threats to their goals and objectives, (2) **assess** the likelihood of these threats materializing and evaluate the impact such an occurrence would have on the organization's operations, finances, and/or reputation, and (3) **apply a risk response** (e.g., mitigate, transfer, avoid, or accept) to bring the risks to an acceptable level.

Cyber risk management focuses on safeguarding systems and data, ensuring the organization can achieve its goals while navigating the complex landscape of potential threats and vulnerabilities.

Common Misconceptions about Risk!

"Using a Third Party Transfers All Risk"

- *Clarification:* Outsourcing or partnering with third parties may shift responsibility but does not remove all risks. The organization is still accountable for oversight and can still be impacted if a risk were to materialize.

"Risk Management is Only About Cybersecurity"

- *Clarification:* Risk management includes financial, operational, legal, reputational, and other risks—not just cyber risks.

“Risk Management is a One-Time Effort"

- *Clarification:* Risk management is an ongoing process that evolves with new threats, business changes, and external factors.

"Low Likelihood Means Low Concern"

- *Clarification:* Even low-likelihood risks (e.g., rare disasters) can have high impact and must be accounted for.

Risky Business with a Twist!

- What is a risk? It's like walking on a tightrope while juggling flaming swords!- Anything that could adversely impact your goals, objectives, and mission.
- Risk Appetite: Think of it as a buffet where you only grab the food you can afford to lose!
- Risk Tolerance: It's the acceptable level of 'oops' you can handle before panicking!
- Risk Threshold: The line where fun stops, and the 'uh-oh' begins!
- Residual Risk: The tiny gremlins that stick around even after you've cleaned up your mess!

Values-Driven Approach to Defining Risk

Who are we? What do we do? Why do we do it?

- What sorts of risk might directly affect our mission, tarnish our perception of ourselves, and/or make us not want to come to work any more?

Remember S-FORC:

- Strategic: risks that threaten the core of our mission, our goals, and our objectives?
- Financial: risks that threaten our financial stability?
- Operational: risks that threaten our ability to manage day-to-day functions of the business?
- Reputational: risks that threaten our reputation?
- Compliance: what are our business obligations (contractual requirements and regulatory/statutory obligations) and what happens if we break compliance with those requirements?

Think about what measures are already in place to mitigate these risks?

- Are these controls working effectively? How do we know? Where can we improve?

Risk Management: Why it Matters

- **Protect Critical Operations and Data**
  - Safeguards the systems, data, and processes vital to your organization's mission.
- **Fulfill Business Obligations**
  - Ensures compliance with contractual, legal, and regulatory requirements to avoid penalties and maintain partnerships.
- **Enable Informed Decision-Making**
  - Provides leadership with clarity on risks to balance opportunity and protection effectively.
- **Maintain Financial Stability**
  - Reduces the financial impact of incidents, including fines, lawsuits, and recovery costs.
- **Support Long-Term Resilience**
  - Builds a foundation for adapting to new risks and challenges without derailing town objectives.

How Risk Management Works

The risk management lifecycle is a continuous process designed to identify, assess, and address risks effectively. Each step plays a vital role in ensuring risks are managed holistically.

1. Risk Identification
- Recognize potential risks that could impact objectives, operations, or assets.

2. Risk Analysis
- Assess the likelihood and impact of identified risks to prioritize mitigation efforts.

3. Risk Mitigation Planning
- Develop strategies to reduce, transfer, or accept risks based on their severity.

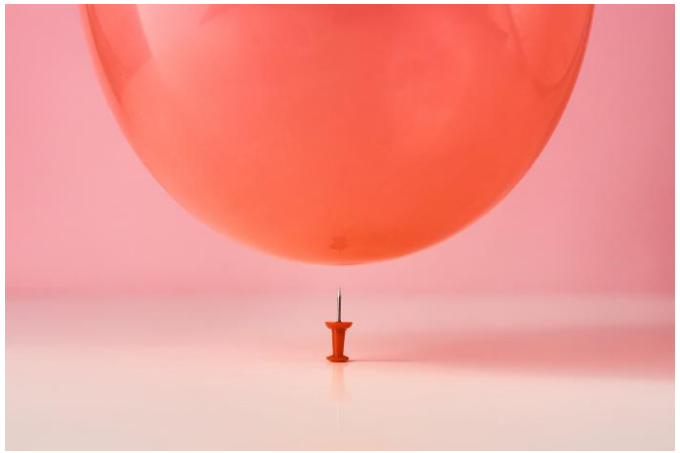
4. Risk Management Implementation
- Execute the planned mitigation measures and integrate them into operations.

5. Review and Tracking
- Continuously monitor risks and review the effectiveness of mitigation strategies to adapt as necessary.

When should you assess risk?

- When you are thinking about a new “thing”. How many folks are looking at AI use?
- When something big changes or is about to change. Think mergers, think new systems, think a new line of business.
- On a regular basis. Annually at a minimum.
- As threats change. You start hearing about new threats in the news or your service provider tries to sell you a new tech product. What’s the risk and how does this thing or change help mitigate this risk?

Assessing & Responding to Risk



Risk Response

Accept—formal decision to not act given the risk at a given time as it falls within the risk tolerance level.

Mitigate—specific actions are identified to reduce risk to an acceptable level.

Transfer—shift some or all responsibility of a risk to a third-party (e.g., insurance provider, backup vendor, etc.

Avoid—specific actions taken to eliminate the activities or technologies which are the basis for this risk.

A Word on Business Obligations

What Are Business Obligations?

- Commitments the organization must meet, such as:
  - **Legal:** Compliance with any applicable regulatory requirements.
  - **Contractual:** Meeting client agreements.
  - **Ethical:** Organizational or professional mandates for behavior.
- Obligations directly effect financial, operational, and reputational stability.

Why Document Business Obligations?

Identify Risks: Non-compliance risks can have cascading impacts across operations.

Support Prioritization: Understanding obligations helps allocate resources effectively to mitigate high-impact risks.

Inform Strategy: Aligns compliance efforts with risk appetite and tolerance to support decision-making.

Facilitate Better Decision-Making: Creates a foundation for informed business decisions by providing visibility into critical obligations.

Business Obligation Worksheet

Risk Severity: Likelihood & Impact

Likelihood event will take place (L)	Impact of Event (I)					
		Negligible (1)	Marginal (2)	Significant (3)	Critical (4)	Catastrophic (5)
	Very High (>90%) (5)	6	7	8	9	10
	High (61-90%) (4)	5	6	7	8	9
	Possible (41-60%) (3)	4	5	6	7	8
	Unlikely (11-40%) (2)	3	4	5	6	7
	Improbable (1-10%) (1)	2	3	4	5	6

- Avoid
- Avoid / Transfer
- Transfer / Mitigate
- Mitigate
- Mitigate / Accept
- Accept

- How do we establish Severity? Likelihood and Impact.
- Likelihood can be quantified as percentage that the risk is likely to occur.
- If something will catastrophically impact the organization and is very likely to occur, that is a risk that must be treated.

Defining Risk Impact

#	Impact	Range of Monetary Loss if Risk manifests (Impact*)	Range of labor hours loss if Risk manifests (Impact*)	Comments
1	Negligible	< $10,000	< 80	Absorbed into cost of business
2	Marginal	$10,001 up to $100,000	81 up to 400	Risk threshold – Up to $1M Risk threshold – Up to 2,000 hours Risk Tolerance - $10k – $1M Risk Tolerance – $80 – 2,000 hours
3	Significant	$100,001 up to $500,000	400 up to 1,000	
4	Critical	$500,001 up to $1,000,000	1,001 up to 2,000	
5	Catastrophic	> $1,000,000	> 2,000	Unacceptable—Treat the risk or avoid if likelihood of occurrence is very high.

Think about Transference

Understand: Impact can be *quantitative* and *qualitative*; everything besides human safety or loss of life boils down to how much time and money are you willing to spend!

Risk Elicitation

What do we need to protect?

- What are the important things we use in our organization? Think- data, not just tools.
- Of these things, which ones are most important?

What could go wrong?

- What might happen to these important things?
- Are there any problems with our computers or how we do things that could make it easier for bad things to happen?

How bad would it be if something went wrong?

- What would happen if we lost or someone stole, or altered these important things?
- How much trouble would it cause for our work and our reputation?
- What are some potentially impactful events that keep you up at night?

What are we doing to keep things safe?

- What are the ways we already use to protect our important stuff?
- Do these ways actually work well?

Risk Elicitation (cont.)

How likely is it that something bad will happen?

- Is it very likely, somewhat likely, or not likely at all that the bad things we thought about will actually happen?
- Has anything like this happened to us before? And if something did happen in the past, has it been addressed sufficiently to keep it from happening again?

How much trouble would it cause if something bad did happen?

- If one of the bad things we thought about actually happened, how much of a mess would it make for us?
- Would it be a little problem, a big problem, or a huge disaster?

Which problems should we worry about the most?

- Out of all the bad things we talked about, which ones should we really focus on fixing first?
- Are there any that we need to fix right away?

Risk Elicitation Exercise

Cyber Insurance and Risk Management

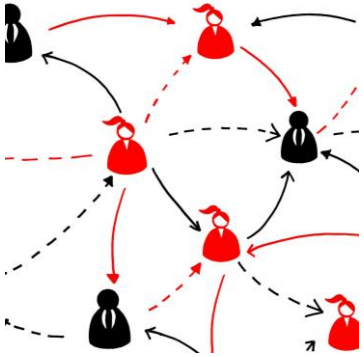
Understanding Cyber Insurance Coverage

Coverage for Data Breaches

Cyber insurance provides coverage for expenses resulting from data breaches, including costs for legal representation and notifications.

Legal Fees and Costs

One of the key benefits of cyber insurance is compensation for legal fees incurred during data breach incidents.



Public Relations Efforts

Cyber insurance can assist with public relations efforts to mitigate damage and protect an organization's reputation after a breach.

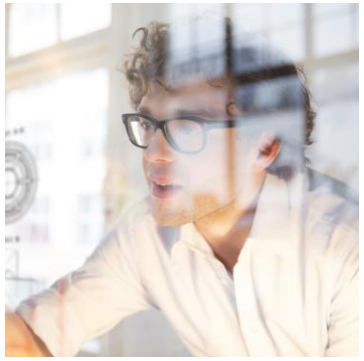
How Cyber Insurance Can Mitigate Financial Impact

Reducing Financial Burden

Cyber insurance helps organizations mitigate the financial impact of cyber incidents, providing essential support during crises.

Resource for Recovery

Cyber insurance offers vital resources and support for businesses to recover quickly from cyber incidents and breaches.

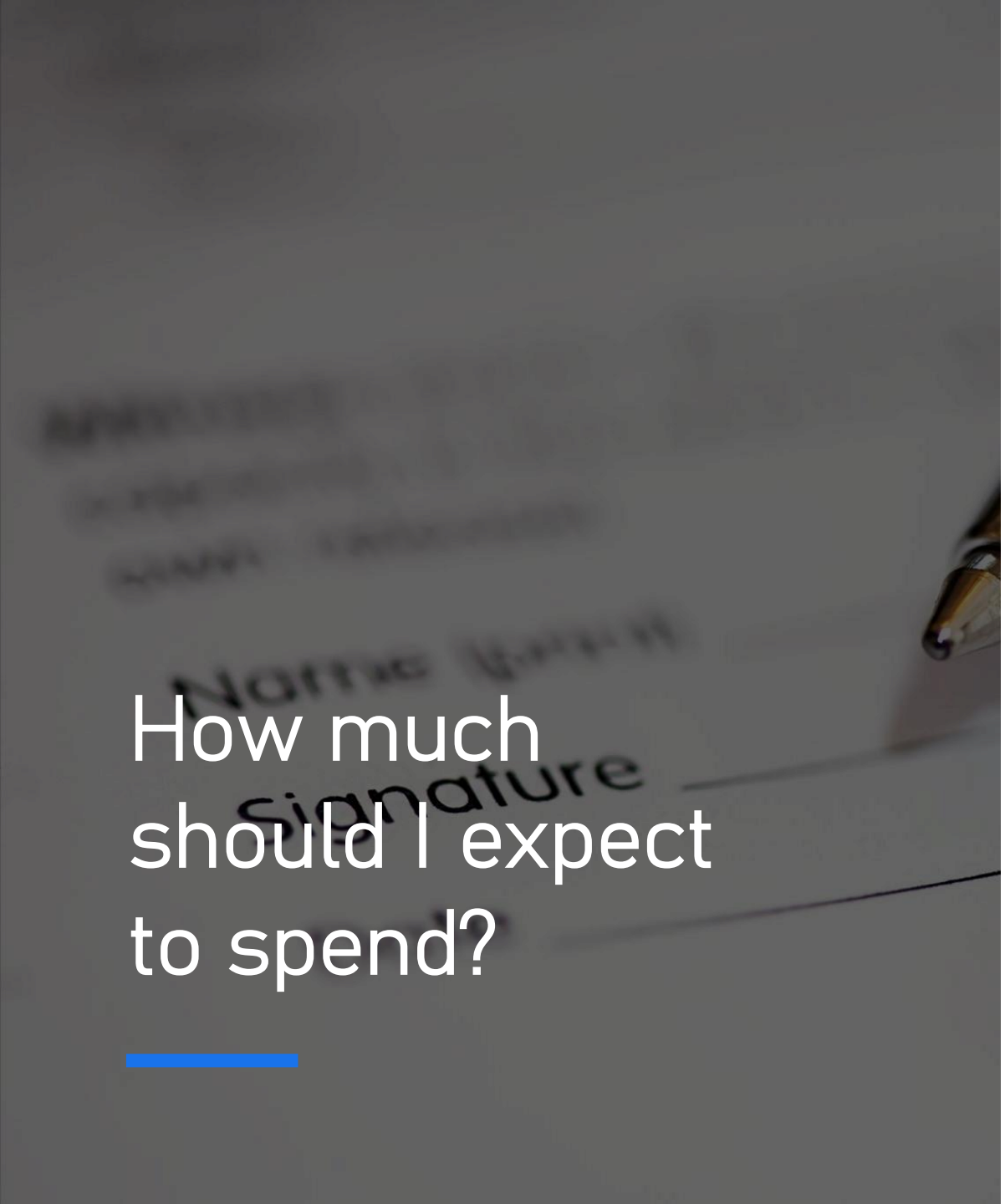


Maintaining Operational Continuity

Having cyber insurance helps organizations maintain operational continuity, minimizing downtime and disruptions caused by cyber threats.

What does a "good" policy look like?

Coverage	CLAIM LETTER	EXAMPLE
Aggregate Limit	$1,000,000	$1,000,000
Deductible	$0	Example
Premium	????	Example
Third Party Coverages		
Privacy and Security Liability	$50,000	$1,000,000
Regulatory Fines and Penalties	NOT INCLUDED	$1,000,000
Notification Costs	$50,000	$1,000,000
PCI Fines and Assessments	NOT INCLUDED	$1,000,000
Multimedia Liability	NOT INCLUDED	$1,000,000
First Party Coverages		
Breach Response Expenses	$50,000	$1,000,000
Ransomware & Extortion Loss	$50,000	$1,000,000
Data Replacement and Recovery	NOT INCLUDED	$1,000,000
Public Relations	$50,000	$1,000,000
Business Interruption	NOT INCLUDED	$1,000,000
Reputation Damage	NOT INCLUDED	$1,000,000
Dependent Network Interruption	NOT INCLUDED	$1,000,000
Dependent System Failure	NOT INCLUDED	$1,000,000
Hardware Replacement Costs/Betterment	NOT INCLUDED	$1,000,000
Crime Coverages		
Electronic Theft (Funds Transfer)	$20,000	$100,000-$250,000
Social Engineering	NOT INCLUDED	$100,000-$250,000
Invoice Manipulation	NOT INCLUDED	$100,000-$250,000
Telephone Fraud	NOT INCLUDED	$100,000-$250,000
Cryptojacking	NOT INCLUDED	$100,000-$250,000



How much should I expect to spend?

Premiums are based on a number of factors, including revenue

Your “Business Obligations” are another. HIPAA covered entity? Expect to pay more.

Security controls reduce risk and premium, allowing your organization to be in front of more insurance carriers. Competition reduces rates.

Most $1,000,000 aggregate policies are between $2000 and $8000 for annual premium.

How do I get insured and save money on my insurance?

The path to cyber insurability

Step 1: Understand Your Risk

Why it matters: Knowing where you're vulnerable helps you fix problems before they happen and shows insurers, you're serious about security.

Key action: Identify your biggest risks and write them down. Focus on your most important systems and data.

Step 2: Know Your Assets

Why it matters: You can't protect what you don't know you have. Insurers expect you to keep track of your systems, data, and devices.

Key action: Make a list of your computers, software, and sensitive data. Keep it updated.

8 Cyber insurance essentials

Multi-Factor Authentication (MFA)

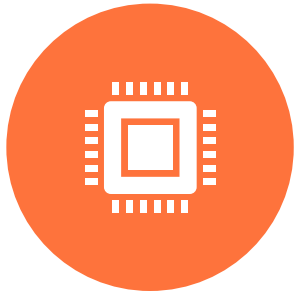
Why it matters: Stops hackers from getting in even if they steal a password.

Key action: Turn on MFA for email, sensitive systems, and anything used remotely.

Backup and Recovery

Why it matters: Ensures you can recover your data if something goes wrong, like ransomware.

Key action: Back up your data regularly and test that you can restore it.



Endpoint Detection and Response (EDR)

Why it matters: Helps you quickly find and stop cyber threats on your computers.

Key action: Use tools to monitor and respond to suspicious activity on devices.

Email Filtering

Why it matters: Blocks dangerous emails that could trick employees or spread malware.

Key action: Use email filters to catch phishing and malicious emails before they reach inboxes.

8 Cyber insurance essentials

Patch and Vulnerability Management

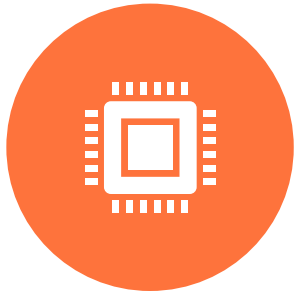
Why it matters: Fixes weak spots in your software before hackers exploit them.

Key action: Regularly update your systems and software.

Security Awareness Training

Why it matters: Employees who recognize cyber threats make fewer mistakes.

Key action: Train your staff on spotting phishing emails and other scams.



Incident Response Plan

Why it matters: Having a plan reduces chaos and speeds up recovery during a cyberattack.

Key action: Write down what to do if there's an attack and practice the plan.

Funds Transfer Policy

Why it matters: Prevents fraud by requiring checks before transferring money.

Key action: Always double-check large payments with multiple people..

Actionable Strategies for Cyber Protection

Developing a Comprehensive Cyber Security Plan

Security Policies

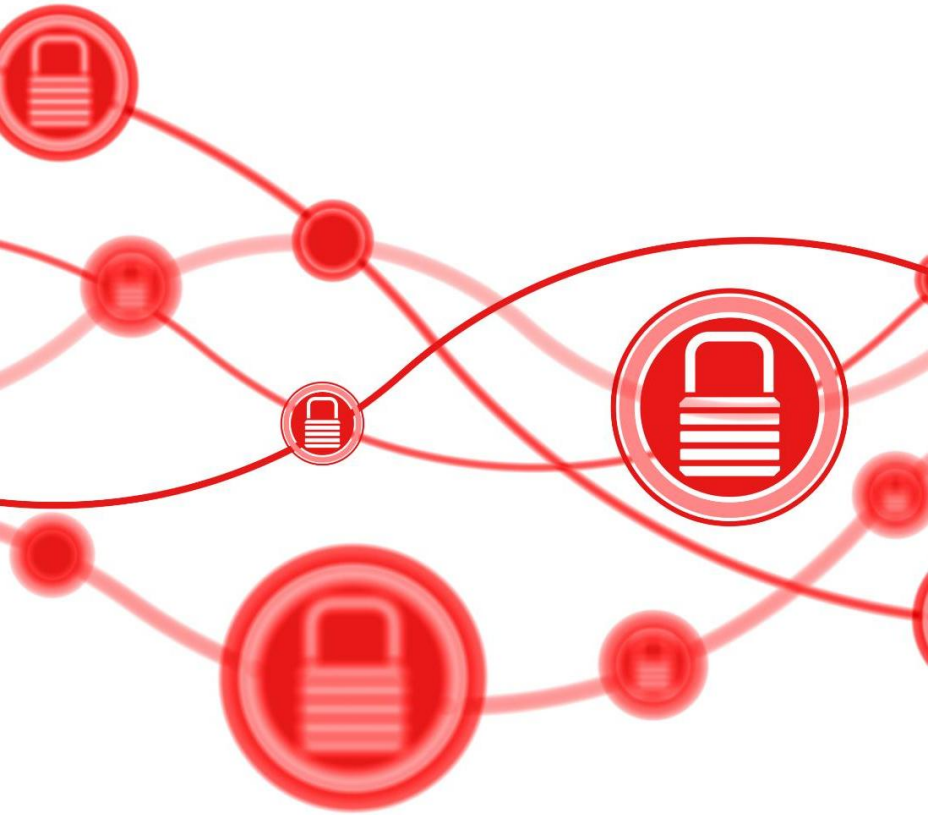
Establishing clear security policies is essential for guiding employees' actions and protecting organizational assets.

Response Procedures

Developing effective response procedures ensures quick action during security incidents to minimize damage and restore normal operations.

Proactive Risk Management

A proactive approach to risk management involves identifying potential threats and vulnerabilities before they escalate into significant issues.



Practical Tools and Resources for Nonprofits

Security Software

Nonprofits should invest in security software to safeguard their sensitive information from cyber threats and data breaches. Check out the Microsoft donation program at Techsoup.org. The Business Premium plan for Microsoft 365 has just about everything needed for the foundation of a modern security program

Training Programs

Implementing training programs for staff can significantly improve awareness and skills related to cybersecurity best practices.

Resource Accessibility

Utilizing accessible resources helps nonprofits stay informed about the latest cybersecurity threats and defense strategies. What are some of your go to resources for cyber security?

Conclusion

Evolving Cyber Threats

Cyber threats are constantly changing, making it essential for nonprofits to stay informed and proactive in their cybersecurity measures.

Prioritizing Cybersecurity

Nonprofits must prioritize cybersecurity to protect sensitive data and resources essential for their operations and mission.

Effective Communication

Communicating with stakeholders about cybersecurity is vital for building trust and ensuring collaborative efforts in safeguarding resources.

Q & A

Greg Bugbee, CISSP

Chief Information Security Officer

gbugbee@novusinsight.com