whitleypenn

Beyond the Breach: Leadership in Cyber Cleanup

JESUS VEGA, CISSP

Agenda

- Understanding Cybersecurity Breaches
- Immediate Response: What Leaders Must Do
- Legal, Regulatory & Notification Requirements
- Managing Public Perception & Stakeholder Communication
- Proactive Leadership: Building Resilience
- Preventative Measures

About Whitley Penn

Whitley Penn is the 35th largest firm in the nation based on 2024 rankings in *Accounting Today,* 35th in the nation based on 2024 rankings in *INSIDE Public Accounting's* "Top 100 Firms", 20th in the nation based on 2024 - 2025 rankings from VAULT ACCOUNTING 25, and one of the fastest growing firms in the nation. We have an extensive team of experienced audit, tax, consulting, and valuation professionals that we will be able to draw upon as needed.

whitleypenn

Our Services

- Audit
- Consulting
- Forensic, Litigation & Valuation
- Client Accounting & Advisory Services
- Risk Advisory Services
- Cybersecurity Services
- Tax (including International, State, and Local)
- Transaction Advisory Services
- Wealth Management (WPWealth)

whitleypenn

REPORTS & READINESS ASSESSMENTS

System and organizational control reports and assessments provide you with an opportunity to affirm the design and effectiveness of your internal controls for all the data you process or store on your clients' behalf. Whitley Penn's solutions include multiple industry-tailored SOC report options, SOC readiness assessments, and SOC 2+ HITRUST assessment reports.

WHICH REPORT OR ASSESSMENT IS RIGHT FOR YOU?

SOC Readiness Assessments

An evaluation of the organization's current state to identify any gaps that need to be remediated prior to a SOC examination.

SOC 1

Allows you to demonstrate to your clients and their auditors that the internal control over their financial data is effective and in compliance with laws and regulations, such as Sarbanes-Oxley 404.

SOC 2

Provides your clients with information on your controls over the security, availability, processing integrity, confidentiality, and privacy of their data (Trust Services Criteria).

Cybersecurity Risk Assessments

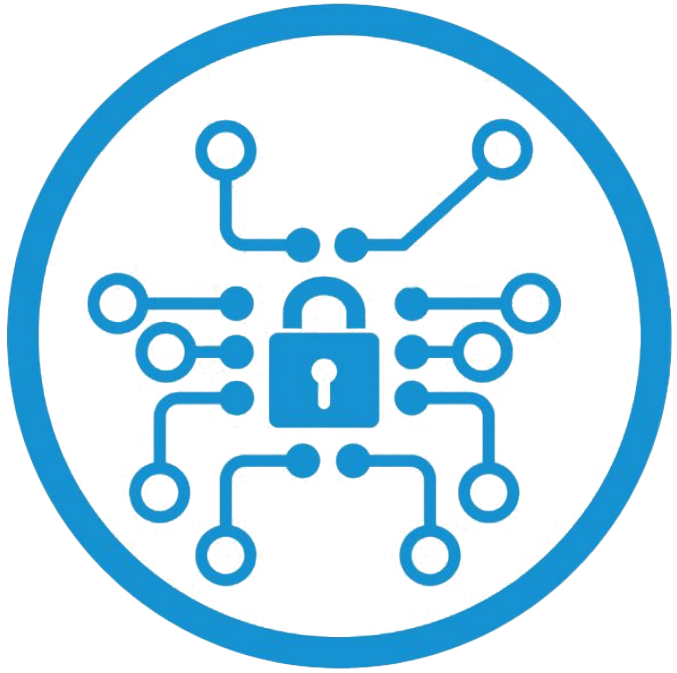
- The goal is to protect the organization from cyber threats, ensure compliance with regulations, and maintain business continuity. This process is crucial in today's digital world where cyber threats are increasingly sophisticated and pervasive.

CISO Advisory

- Fractional CISO services provide organizations with access to experienced Chief Information Security Officer (CISO) expertise on a part-time or as-needed basis. This is particularly beneficial for organizations that may not have the resources or need for a full-time CISO.

Penetration Testing

- Our penetration testing services emulate real-world attacks from "hackers" and highlight areas needing improvement and/or additional investment.



Understanding Cybersecurity Threats

Attack Vectors

Phishing

Ransomware

Vendor Compromise

Insider Threats

Phishing

Phishing attacks are the most common method that cybercriminals use to gain access to an organization's network. They take advantage of human nature to trick their target into falling for the scam that usually entails creating a sense of urgency.

Tips for identifying attempted attacks, including:

- Do not trust unsolicited emails
- Do not send any funds to people who request them by email, especially not before checking with leadership
- Always filter spam
- Configure your email client properly
- Do not click on unknown links in email messages
- Beware of email attachments. Verify any unsolicited attachments with the alleged sender (via phone or other medium) before opening it
- Remember that phishing attacks can occur over any medium (including email, SMS, enterprise collaboration platforms and so on)

Ransomware

Should you open that email attachment?

- If it's suspicious, delete and don't open it!
- What is suspicious?

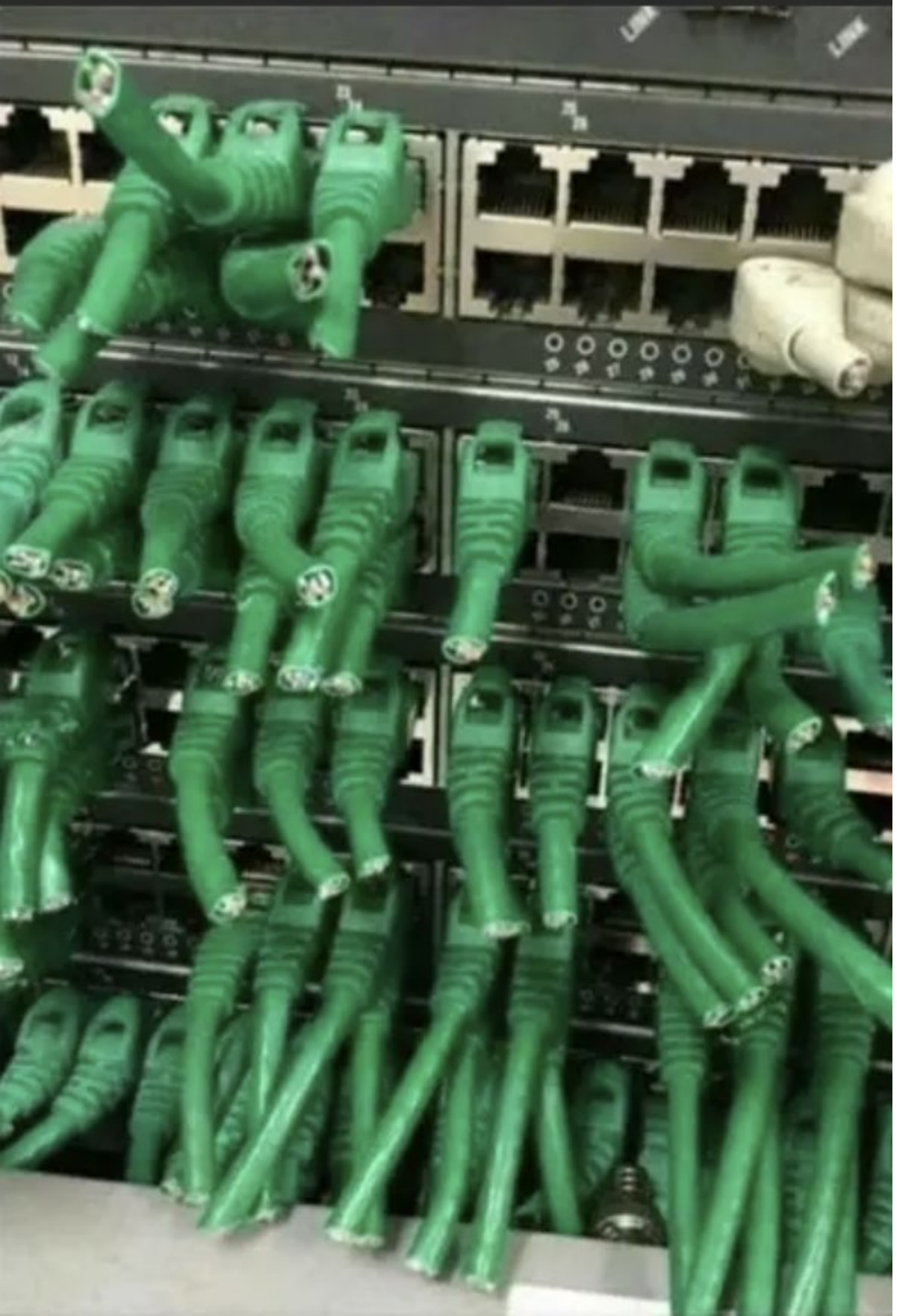
Vendor Compromise

Criminals are targeting vendors to go after customer funds and data.

Vendors that have access to an entity's information systems must be monitored and controlled.

Several cases have been reported whereby vendors are compromised with the intent of stealing funds and data from the vendor's customers.

Contract review, right to audit, and monitoring of vendor performance are critical to securing vendor access to your data.



Insider Threats

Disgruntled Employee. Someone who deliberately causes harm to the organization's digital infrastructure. For instance, a former IT staff member who still has access to internal systems might log in and alter the configuration of the company's website

Unintentional Insider threat. Can occur when an employee with access to critical systems, like a web administrator or developer, misconfigures a company website

hello! Please send help for our files
HIDE ? 14 days ago

Hello, this is ContiLocker Team.
Please, introduce yourself (Company name and your position) and we'll provide all necessary information.
Sometimes our staff is busy, but we will reply as soon as possible.
HIDE 14 days ago ✔

Our network is the Broward County Public School network? is this where we get our files back? please tell me what to do next
HIDE ? 14 days ago

What happened? The bad news is that we hacked your network and encrypted your servers, as well as downloaded more than 1 terabyte of your personal data, including financial, contracts, databases and other documents containing SSN addresses DOB and other information about students and teachers.
If this data is published, you will be subject to huge court and government fines.
The good news is that we are businessmen. We want to receive ransom for everything that needs to be kept secret, and don't want to ruin your reputation.
The amount at which we are ready to meet you and keep everything as collateral is $40,000,000.
HIDE 14 days ago ✔

I am...speechless. Surely this is a mistake? are there extra zero's in that number by mistake?
HIDE ? 14 days ago

According to the records, your revenue is more than 4billions. So it is a possible amount for you.
We also made a research to throw your finance and know that you own the required amount.
HIDE 14 days ago ✔

i am so confused. this is a PUBLIC school district. public, meaning it is free for students to attend. You cannot possibly think we have anything close to this!
HIDE ? 14 days ago

What is your position?
HIDE 14 days ago ✔

Cyber Fraud Financial Impact

Cybercrime to cost the world $10.5 Trillion in 2025

$9.36M average cost of US breach

- This cost does not include ransomware payments

Cost Breakdown of a Cyber Fraud Breach

Category	% of Total Cost	Estimated Cost (USD)
Lost Business	~38%	~$3.56 million
Detection and Escalation	~29%	~$2.71 million
Post-Breach Response	~27%	~$2.53 million
Notification Costs	~6%	~$560,000

About Ingram Micro

- Headquarters: Irvine, California, USA
- IT Resellers and VARs (Value-Added Resellers)
- Managed Service Providers (MSPs)
- System Integrators
- Independent Software Vendors (ISVs)
- Large Enterprises and SMBs
- Public Sector Organizations
- Annual Revenue (2024): Approx. $48.9 billion
  - NYSE: INGM

Ingram Micro cybersecurity breach

Timeline:

- July 3, 2025: Core systems went offline early in the morning.
- Later that day: Customers reported that online ordering systems and websites were unresponsive.
- July 4: Systems were shut down, and employees were instructed to work from home.
- July 5: Ingram Micro publicly confirmed the ransomware attack in a press release.
- July 6–8: Partial recovery began, with some systems like the website coming back online, though order and licensing systems remained down
- July 9: All system recovered

whitleypenn

Greetings! Your corporate network was attacked by Safepay team.
Your IT specialists made a number of mistakes in setting up the security of your corporate network, so we were able to spend quite a long period of time in it and compromise you.
It was the misconfiguration of your network that almost allowed our experts to attack you, this situation is simply as a paid training session for your system administrators.
We've spent the time analyzing your data, we know the ins and outs of your corporation. As a result, all files of importance have been encrypted and the ones of most interest to us have been stolen and are now stored on a secure server for further publication on the web with an open access.
We have in possession on your files, such as financial statements, intellectual property, accounting records, lawsuits and complaints, personnel and customer files, as well as files containing information on bank details, transactions and other internal documentation.
Furthermore we successfully blocked most of the servers that are of vital importance to you, however upon reaching an agreement, we will unlock these as soon as possible and your employees will be able to continue working.
We are suggesting a mutually beneficial solution to that issue. You submit a contact request and we keep the fact that your network has been compromised a secret, delete all your data and provide you with the key to decrypt all your data. WE ARE THE ONES WHO CAN CORRECTLY DECRYPT YOUR DATA AND RESTORE YOUR INFRASTRUCTURE IN A SHORT TIME. DO NOT TRY TO DECRYPT YOUR FILES YOURSELF, YOU WILL NOT BE ABLE TO DO THIS, YOU WILL DAMAGE THEM AND NO ONE WILL BE ABLE TO RESTORE THEM.
In the event of an agreement, our motivation is a guarantee that all conditions will be fulfilled. No one will ever negotiate with us later on if we don't fulfill our part and we recognise that clearly! We are not a politically motivated group and want nothing more than monetary reward. Provided you pay, we will honour all the terms we agreed to during the negotiation process.
In order to contact us, please use the chat below, you have 7 days to contact us, after this time a blog post will be made with a timer for 3 days before the data is published and you will no longer be able to contact us.

How it happened

- Ingram Micro incident has been attributed to SafePay, a centralized ransomware operation that develops and deploys its own tools.
- SafePay Modus Operandy (M.O.) is to gain entry through VPN credential theft, disables endpoint protection and executes encryption alongside data theft in a double extortion play
- Sources have told BleepingComputer that it is believed the threat actors first gained access to Ingram Micro's network through the company's GlobalProtect VPN platform, likely using compromised credentials gaining access as far back as November

How it happened (continued)

Palo Alto Networks share the following statement with BleepingComputer regarding our reporting that it is believed the threat actors gained access through Ingram Micro's VPN gateway.

"At Palo Alto Networks, the security of our customers is our top priority."

"We are currently investigating these claims. **Threat actors routinely attempt to exploit stolen credentials or network misconfigurations to gain access through VPN gateways**."

Was this preventable?

- This attack may have been blocked at multiple points:
- Access Could Have Been Stopped with consistent multifactor authentication and zero trust policies
- Suspicious Activity Could Have Been Flagged by endpoint detection tools
- Vulnerabilities Could Have Been Found Sooner through regular risk assessment exercises

Ingram Micro Incident Response Plan (IRP)

- Ingram Micro acted quickly.
- Six days from start of incident to recovery
- It shut down systems, reset credentials, enforced multifactor authentication and worked with outside experts.

- Good example of IRP in action
- Detection
  - July 3 first evidence of breach
- Containment
  - July 4 Systems are shut down
  - Third party forensic company support
- Eradication & Recovery
  - Systems are restored from backups
- Communication
  - July 5 Press release informing public of breach

Contingency Planning Process

National Institute of Science and Technology (NIST) Special Publication 80034 Revision 1 Contingency Planning Guide

- Develop the Contingency Planning Policy Statement: Establishes the foundation for the contingency planning program.
- Conduct the Business Impact Analysis (BIA): Identifies and prioritizes critical systems and components.
- Identify Preventive Controls: Measures to reduce the effects of system disruptions.
- Create Contingency Strategies: Develops strategies for system recovery.
- Develop an Information System Contingency Plan: Detailed plan for system recovery.
- Ensure Plan Testing, Training, and Exercises: Validates the plan through regular testing and training.
- Ensure Plan Maintenance: Keeps the plan current and effective.

SEC Cybersecurity Breach Notification

Companies must disclose any material cybersecurity incidents

- Whether a company loses a factory in a fire — or millions of files in a cybersecurity incident — it may be material to investors," said SEC Chair Gary Gensler

- You have **four business days** to disclose a material cybersecurity incident to the SEC after determining that the incident is material. This disclosure must be made on Form 8-K.

SEC Cybersecurity Breach Notification 8-k

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 8-K

CURRENT REPORT
Pursuant to Section 13 or 15(d)
of the Securities Exchange Act of 1934

Date of Report (Date of Earliest Event Reported): July 5, 2025

INGRAM MICRO HOLDING CORPORATION

(Exact Name of Registrant as Specified in its Charter)

Delaware	001-42384	86-2249729
(State or other jurisdiction of incorporation)	(Commission File Number)	(I.R.S. Employer Identification Number)

3351 Michelson Drive, Suite 100, Irvine, CA 92612
(Address of Principal Executive Offices) (Zip Code)

Registrant's telephone number, including area code: (714) 566-1000

Disclosing a breach to the Payment Card Industry (PCI),

Preserve Evidence: Ensure that evidence is preserved for investigation.

Notify Payment Card Brands: Inform the relevant payment card brands (e.g., Visa, MasterCard) as soon as possible - PCI does not define the “as soon as possible”

Notify Acquires: A PCI acquirer, also known as an acquiring bank, is a financial institution that processes credit and debit card transactions on behalf of merchants

Engage a PCI Forensic Investigator (PFI)

Document the Incident: Keep detailed records of the breach, including the nature of the incident, the response actions taken, and the outcomes

Analyze the Incident: Conduct a post-incident review to understand what happened and how it can be prevented in the future.

Other Breach notification requirements

CCPA Breach Notification Requirements

Immediate Notification: Businesses must notify affected California residents and the California Attorney General (if more than 500 residents are affected) as soon as possible

Notify affected consumers and the California Attorney General

VS

GDPR Breach Notification Requirements

72 Hours: Data controllers must notify the relevant supervisory authority within 72 hours of becoming aware of a personal data breach

Notify the affected individuals and Supervisory Authority

> Art. 55 ….. accordance with this Regulation on the territory of its own Member State.

Legislative and Legal Scrutiny

- Potential Data Privacy Violations
  - While Ingram Micro has not yet confirmed a data breach, law firms like are investigating whether personally identifiable information (PII) was compromised
- State data breach notification laws (e.g., California Consumer Privacy Act – CCPA)
  - Federal Trade Commission (FTC) enforcement for unfair or deceptive practices
  - International laws like GDPR if EU data subjects were affected
- Contractual and Regulatory Compliance
  - As a major IT distributor, Ingram Micro may have contractual obligations with vendors and partners that include cybersecurity clauses.
  - Breach of these terms could lead to civil liability or regulatory penalties.

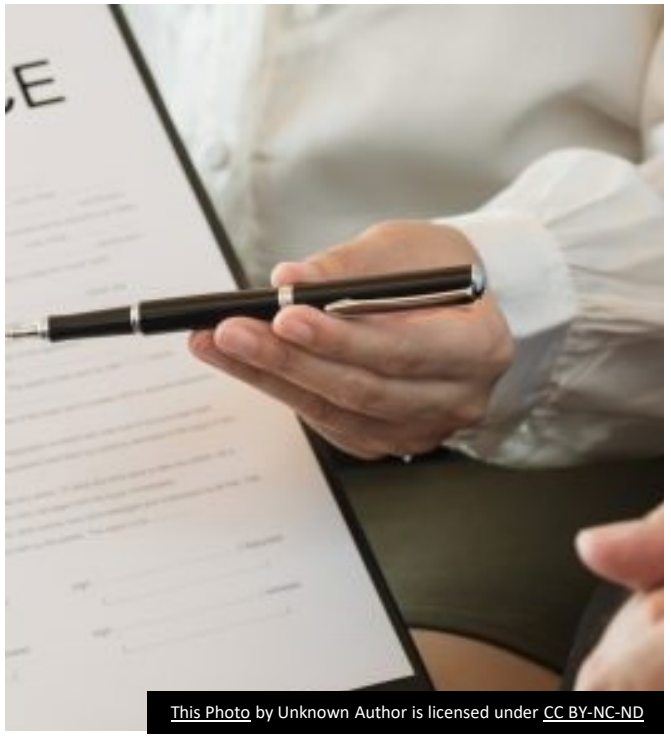
Cyber-insurance

What is cyber-insurance?

- Cyber-insurance protects businesses from financial losses due to cyber incidents like data breaches and ransomware attacks. It covers costs for data recovery, legal fees, business interruption, and damages to third parties.

Cyber-insurance typically covers

- Data Breaches
- Ransomware attacks
- Business interruption
- Cyber Extortion
- Legal expenses
- Data recovery
- Forensic Investigations



Cyber-insurance

Ingram Micro **likely** leveraged its cyber insurance

- Business interruption losses
  - $136 million/day in lost revenue during downtime
  - suggesting potential total losses of $500–$680 million in revenue alone.
    - *source International Business Times
- Third-party liability if customer or partner data was compromised
  - No confirmation of exposed client data
    - At risk data:
      - Order information
      - Vendor and channel partner cost information
      - Logistics information

Impact to their coverage

- Raise in premiums
- Higher deductibles
- Limit coverage on misconfigured infrastructure
- Provider may require hardened infrastructure

Public Relations

- Reputation Damage
  - Critics emphasized that Ingram Micro sells cybersecurity solutions—yet failed to protect its own systems, which undermines trust in its products and services
  - "Ingram Micro's Response Was Fast But Not Preventive" Frobes article "Three Breaches In Three Weeks: A Wake Up Call For Enterprise Security"

- Pre-breach: The stock was performing steadily with a strong Q1 earning call

- Post-breach (July 5–10, 2025):
- The stock dipped 1.56% in the immediate aftermath of the breach.
- Analysts noted that the quick containment and recovery helped limit long-term investor panic

Public Relations (continued)

- No public backlash from named clients has been reported in the media.
- The company itself acknowledged in its official statement that the incident caused disruptions to customers, vendor partners, and stakeholders, and it issued an apology for the inconvenience
  - Immediate Containment and Mitigation
  - Engaged third-party cybersecurity experts to investigate and remediate the breach
  - Transparent Communication
  - Client Support and Relationship Management
    - not detailed publicly, it is likely Ingram Micro has:
    - Activated dedicated client support teams to handle urgent issues.

Managing public relations (PR) during a cybersecurity breach

Respond Quickly and Honestly

Clear and Concise Communication

Public Pathway for Communication

Apologize and Take Responsibility

Outline Mitigation Strategies

Post-Incident Review

Cybersecurity: A Strategic Business Priority

Cybersecurity has become a significant part of the risk landscape.

- **Financial Impact**: Cyber attacks can lead to substantial financial losses from remediation costs, lost revenue, regulatory fines, and potential lawsuits.
- **Reputation**: A breach can damage your organization's reputation, resulting in loss of customers or business opportunities.
- **Business Continuity**: Cyber attacks can disrupt business operations, impacting revenue and customer trust.

Develop a Cybersecurity Risk Assessment Process

Take inventory of the types of sensitive data and where they are located.

Know what information warrants protection based on law (PII, IP, bank/cardholder data, etc.).

Commitments to customers, vendors, and business partners.

Laws and regulations to which the entity is subject (including breach notification laws).

Benefits of Performing a Risk Assessment

Identify Vulnerabilities

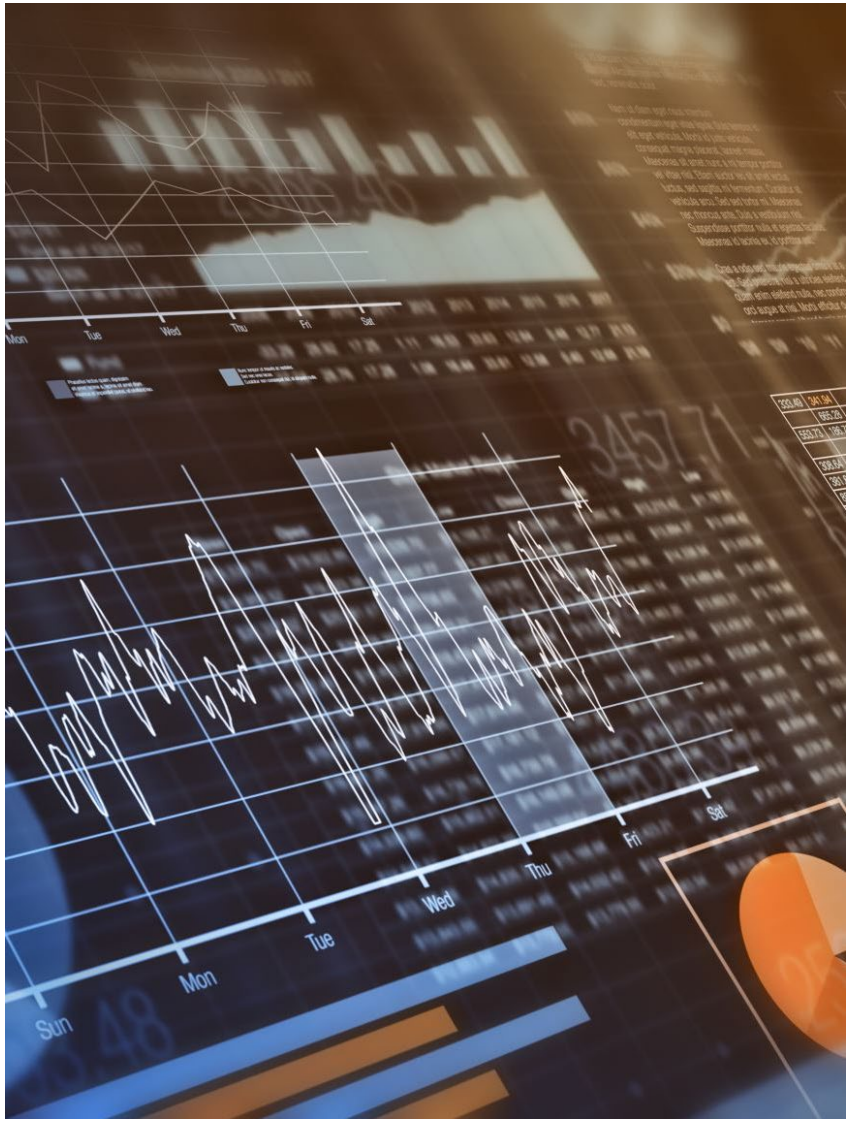
- Cybersecurity risk assessments help organizations identify vulnerabilities in their systems and networks, enabling them to implement controls to prevent cyber incidents.

Compliance with Regulations

- Many industries have regulations that require cybersecurity risk assessments. Performing these assessments helps ensure compliance and avoid potential fines or penalties.

Prioritize Cybersecurity Investments

- By identifying the most significant cybersecurity risks, organizations can better allocate their resources to areas where they are most needed.



Cybersecurity Risk Management

Monitor the Effectiveness of Your Cybersecurity Risk Management Program

- Ongoing and periodic evaluations of the operating effectiveness of controls.
- Internal audit, IT audit, vulnerability scanning/pen testing.
- Review our current backup strategy and the frequency of testing to ensure resilience against data loss and downtime
- Transparency and reporting of any deficiencies in internal controls to those charged with governance.
- Security Awareness Training
- SOC Reporting & 3rd Party Risk.

Internal Control Best Practices

- Segregation of duties
- Incident response planning and testing
- Understanding and evaluating ***third-party risk***
- Segregate critical systems from non-critical systems
- Vulnerability and patch management
- Access management

Contact Information

Jesus Vega
Cybersecurity Managing Director
Jesus.Vega@whitleypenn.com