MEET OUR SPEAKERS

RESEARCH OUR EXPERTISE

SBS Institute
www.sbscyber.com/sbsinstitute/
sbsinstitute@sbscyber.com
605.269.0909

ABOUT US

Welcome to the SBS Institute

Jon Waldman, CISA, CRISC
President, SBS Institute

At SBS CyberSecurity, we strongly believe in the power of education and security awareness training when it comes to creating a strong Information Security Program. To assist organizations with creating a culture of cybersecurity, we created the SBS Institute.

The SBS Institute is a leading provider of cybersecurity education in the financial industry; offering webinars, onsite seminars, conference speaking, and employee or customer training to increase awareness and knowledge around cybersecurity risks.

We have also created a unique series of role-based cybersecurity certifications that provide industry-specific information security awareness and risk management skills to employees that will create confidence with examiners and auditors.

Our talented speakers and instructors have been a part of hundreds of events from coast to coast. We are passionate about sharing our cybersecurity knowledge to help make organizations more secure. Thank you for considering the SBS Institut

WHY SBS INSTITUTE?

- **Banking-Specific**
  Our education is uniquely designed for the banking industry.
- **Growing Community**
  We have issued over 2,000 certifications to professionals in the financial services industry.
- **Nationally Recognized**
  Speakers and instructors have hosted events for learners in states from coast to coast.
- **Real-World Topics**
  Our speakers provide the opportunity to discuss current real-world issue and establish solutions.
- **Collaboration**
  Our learners can collaborate with a cybersecurity expert to build material to implement at their institution.

EVENTS

Types of Presentations and Certifications

TECHNICAL CONFERENCES

Technology Conference

Security Conference

Operations Conference

EXECUTIVE CONFERENCES

Bank Management Conference

Executive Conference

Annual Convention

ONSITE SECURITY AWARENESS TRAINING

All-Employee Training

IT/IS Staff Training

Executive Team/Director Training

Customer/Community Training

HALF/FULL-DAY ONSITE SEMINARS

Cybersecurity

Incident Response

Business Continuity

IT/IS Forum

CERTIFICATION PROGRAMS

Online Course Offering

Onsite Bootcamp (Local or Regional)

"SBS Institute has provided a flexible and comprehensive certification course that offers the custom focus that I was looking for. Great care was taken in the design and execution of this course to ensure that proper emphasis and clarification were used in reviewing the laws and regulations that apply to banking security professionals. Bravo to SBS for delivering high value." – Evan Gottschalk

Event Specialties

- Conferences
- Webinars
- Annual Convention
- Technology and Security Forums
- Round Table/Panel Member
- Onsite Certification and Training

Jon Waldman, CISA, CRISC

Co-founder – SBS CyberSecurity/SBS Institute,
President – SBS Institute, Chief People Officer,
Executive Vice President, IS Consulting – SBS CyberSecurity

Jon Waldman is a co-founder and Execute Vice President of Information Security Consulting for SBS CyberSecurity, as well as SBS' Chief People Officer and the President of the SBS Institute. Over the past 17 years, Jon has helped hundreds of organizations identify and understand cybersecurity risks to allow them to make better and more informed business decisions. Jon is incredibly passionate about cybersecurity training and education, which lead him to be a driving force in the development of the SBS Institute. The Institute is uniquely designed to serve the banking industry by providing industry-specific cyber education. It has grown to include ten certification courses and holds State Association partnerships in over 30 states.

Jon maintains his CISA, CRISC, and CDPSE certifications. He received his Bachelor of Science in Computer Information Systems and his Master of Science in Information Assurance with an emphasis in Banking and Finance Security from Dakota State University, a Center of Academic Excellence in Information Assurance Education designated by the NSA.

Along with being an instructor for SBS Institute courses, Jon frequently speaks on cybersecurity topics at a variety of events and trainings across the country. Additionally, he is a blog author, has had multiple articles published, and regularly hosts educational webinars. Jon strongly believes the more knowledgeable and educated we all are - Directors, employees, and customers alike - when it comes to cybersecurity, the more risk we reduce as a whole.

Learn more about Jon by connecting on LinkedIn.

QUICK FACTS

- Over 15 years of experience helping financial institutions manage cyber risk
- Holds a Master's Degree, as well as CISA and CRISC certifications
- Passionate about cybersecurity training and education
- Frequently hosts webinars and speaks at events across the country sharing his expertise

Event Specialties

- Conferences
- Webinars
- Annual Convention
- Technology and Security Forums
- Round Table/Panel Member
- Onsite Certification and Training

Chad Knutson, CISSP, CISA, CRISC

Co-founder – SBS CyberSecurity/SBS Institute
President and Chief Information Security Officer – SBS CyberSecurity

Chad Knutson is a co-founder and President/Chief Information Security Officer for SBS CyberSecurity. Over the past 15 years, Chad has worked diligently to help hundreds of organizations identify and understand cybersecurity risks to allow them to make better and more informed business decisions.

Chad maintains his CISSP, CISA, and CRISC certifications. He received his Bachelor of Science in Computer Information Systems and his Master of Science in Information Assurance from Dakota State University, a Center of Academic Excellence in Information Assurance Education designated by the NSA.

Chad is dedicated to educating industry professionals about cybersecurity. While consulting with financial institutions, he saw the need to empower employees to be better prepared to confidently handle cybersecurity threats, create and manage strong information security programs, and understand ever-changing regulations. This led Chad to be a driving force in the development of the SBS Institute, where he served as President for seven years. The Institute is uniquely designed to serve the banking industry by providing industry-specific cyber education. It has grown to include ten certification courses and holds State Association partnerships in over 30 states.

Chad is incredibly passionate about cybersecurity training and education for everyone - Directors, employees, and customers alike. He is an instructor for SBS Institute courses, webinar host, and frequently speaks on cybersecurity topics at a variety of events and trainings across the country, including trainings for State Examiners.

Learn more about Chad by connecting on LinkedIn.

QUICK FACTS

- Over 15 years of experience helping financial institutions manage cyber risk
- Dedicated to educating industry professionals
- SBS Institute instructor
- Holds a Master's Degree, as well as CISSP, CISA and CRISC certifications
- Frequently hosts webinars and speaks at events across the country sharing his expertise

Event Specialties

- Conferences
- Webinars
- Technology and Security Forums
- Round Table/Panel Member

Buzz Hillestad, GCFE

Senior Vice President Information Security Consulting - SBS CyberSecurity

Buzz Hillestad is a Senior Vice President, Information Security Consulting at SBS CyberSecurity, where he works to help organizations identify and understand cybersecurity risks to allow them to make better and more informed business decisions. Buzz is passionate about Digital Forensics and Incident Response. He was a driving force in the creation of the SBS DFIR team, which he currently leads.

Buzz received a Bachelor of Computer Information Systems for Business from Dakota State University and has performed Master-level work in Information Security from the SANS Institute – an internationally recognized best source for cybersecurity education - where he has also obtained his GIAC Certified Forensics Examiner certification. He has been involved with information security practice in Healthcare, Banking, Government, and a variety of other industry verticals for over 15 years.

Buzz is dedicated to sharing his cybersecurity, digital forensics, and incident response knowledge. He is an instructor for the SBS Institute certification program, hosts webinars, and conducts trainings. Buzz additionally is a blog author and has had numerous security publications in magazines and speaks nationally on cybersecurity topics.

Learn more about Buzz by connecting on LinkedIn.

QUICK FACTS

- Over 15 years of experience working in cybersecurity
- Holds a Bachelor's Degree in Computer Information Systems from Dakota State University
- Frequently hosts webinars and speaks at events across the country sharing his expertise
- Digital forensics and incident response expert
- Maintains his GIAC Certified Forensic Examiner (GCFE) certification
- SBS Institute instructor
- SBS Consulting Team Regional Director and DFIR Lead

Event Specialties

- Webinars
- Technology and Security Forums
- Round Table/Panel Member
- Onsite Certification and Training

Cody Delzer, CISA

Vice President Information Security Consulting/Regional Director - SBS CyberSecurity

Cody Delzer is a Vice President Information Security Consulting for SBS CyberSecurity, where he works to help organizations identify and understand cybersecurity risks to allow them to make better and more informed business decisions.

Cody maintains his CISA certification and has a Bachelor of Science Degree in Computer and Network Security from Dakota State University, a Center of Academic Excellence in Information Assurance Education designated by the NSA. Since 2011, Cody has assisted financial institutions and other private industry organizations across the United States with a focus on IT and IT security, systems operations, and information assurance.

Cody is an instructor for the SBS Institute certification program, performs speaking engagements, and conducts trainings. He additionally is a blog author, has had multiple articles published, and hosts educational webinars.

Learn more about Cody by connecting on LinkedIn.

QUICK FACTS

- Over 10 years of experience helping financial institutions manage cyber risk
- Holds a Bachelor's Degree in Computer and Network Security from Dakota State University
- SBS Consulting Team Regional Director
- Maintains his CISA and CDPSE certifications
- SBS Institute Instructor
- Frequently hosts webinars and speaks at events across the country sharing his expertise

Event Specialties

- Webinars
- Technology and Security Forums
- Round Table/Panel Member
- Onsite Certification and Training

Shane Daniel, CPA, CISA, CRISC, CIA, CGEIT

Senior Information Security Consultant – SBS CyberSecurity

Shane Daniel is a Senior Information Security Consultant for SBS CyberSecurity, where he works to help organizations identify and understand cybersecurity risks to allow them to make better and more informed business decisions.

As a former community bank internal auditor and compliance officer, Shane has over 25 years of experience helping financial institutions manage risk and profitability. He is driven to be an expert in his field by maintaining a variety of premier industry certifications, including Certified Public Accountant (CPA), Certified Information Systems Auditor (CISA), Certified in the Governance of Enterprise IT (CGEIT), Certified in Risk and Information Systems Control (CRISC), and a Certified Internal Auditor (CIA). Shane specializes in risk management, information technology audit, Bank Secrecy Act independent testing, compliance management, information security, and internal audit outsourcing.

Shane performs speaking engagements, conducts trainings, has had multiple articles published, and hosts educational webinars.

Learn more about Shane by connecting on LinkedIn.

QUICK FACTS

- Over 27 years of experience helping financial institutions manage cyber risk.
- Holds 5 industry certifications
- SBS Consulting Team Regional Director
- Is a Certified Public Accountant (CPA)

Event Specialties

- Webinars
- Technology and Security Forums
- Round Table/Panel Member

Lynda Hartup, CISA, CISM, CBSM

Senior Information Security Consultant – SBS CyberSecurity

Lynda Hartup is a Senior Information Security Consultant at SBS CyberSecurity (SBS), a company dedicated to helping organizations identify and understand cybersecurity risks to make more informed and proactive decisions.

Lynda maintains her Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), and Certified Banking Security Manager (CBSM) certifications. She received her Bachelor of Interdisciplinary Studies from the University of Southern Mississippi and completed the Graduate School of Banking at Louisiana State University.

Lynda has 20 years of financial institution experience in various positions, including Information Security Officer and dedicated IT Examiner. She also served for seven years as a Bank Examiner-IT Specialist for the Mississippi Department of Banking. Her specialties lie in IT governance, risk management, and regulatory compliance.

Lynda is passionate about helping her clients maintain the safety and security of their information and assets.

Learn more about Lynda by connecting on LinkedIn.

QUICK FACTS

- Enjoys working with clients and providing value by breaking down large issues into manageable parts.
- Has worked as a Bank Examiner-IT Specialist for the Mississippi Department of Banking.
- Holds several industry certifications and completed the Graduate School of Banking.

Event Specialties

- Webinars
- Technology and Security Forums
- Round Table/Panel Member
- Onsite Certification and Training

Cole Ponto, CBBCP

Senior Information Security Consultant - SBS CyberSecurity

Cole Ponto is a Senior Information Security Consultant for SBS CyberSecurity, where he works to help organizations identify and understand cybersecurity risks to allow them to make better and more informed business decisions.

Cole has a Bachelor of Science in Computer and Network Security from Dakota State University, a Center of Academic Excellence in Information Assurance Education designated by the NSA. He has over five years of IT auditing, consulting, and information security program development experience.

Cole is an instructor for the SBS Institute certification program, performs speaking engagements, and conducts trainings. He additionally is a blog author, has had multiple articles published, and hosts educational webinars.

Learn more about Cole by connecting on LinkedIn.

QUICK FACTS

- Over 7 years of experience helping financial institutions manage cyber risk
- Holds a Bachelor's Degree in Computer and Network Security from Dakota State University
- SBS Institute instructor
- Maintains his CDPSE certification

Event Specialties

- Webinars
- Technology and Security Forums
- Round Table/Panel Member

Dylan Kreutzfeldt, CBSM, CBSTP, CBCM

Senior Information Security Consultant - SBS CyberSecurity

Dylan Kreutzfeldt is an Information Security Consultant at SBS CyberSecurity (SBS), a company dedicated to helping organizations identify and understand cybersecurity risks to make more informed and proactive decisions. He is also an instructor for the SBS Institute, leading the Certified Banking Security Technology Professional (CBSTP) course and hosting educational webinars, security awareness training, and additional speaking engagements.

Dylan maintains Certified Banking Security Manager (CBSM), Certified Banking Security Technology Professional (CBSTP), and Certified Banking Cybersecurity Manager (CBCM) certifications. He received his Bachelor of Science in Network Security and Administration from Dakota State University.

Dylan joined the SBS team in 2015, holding IT audit and network security roles before transitioning into consulting. He specializes in the implementation and governance of internal cyber controls technical background and his skill set was a driving force in championing the creation of the company's Office 365 testing program.

Dylan is passionate about supporting his clients as they continually strive for increased cyber maturity and growing the relationships he builds along the way.

Learn more about Dylan by connecting on LinkedIn.

CBSM, CBSTP, CBCM certifications

QUICK FACTS

- Values building strong relationships with his clients.
- SBS Institute Instructor
- Excited about sharing his knowledge through cybersecurity training and other educational events
- Has working experience in IT audit and network security.
- Holds a Bachelor's Degree, in Computer and Network Security from Dakota State University
- Maintains his CBSM and CBCM certifications

Event Specialties

- Webinars
- Technology and Security Forums
- Round Table/Panel Member

Laura Zannucci, CISA, CISM, CDPSE

Senior Information Security Consultant - SBS CyberSecurity

Laura Zannucci is an Information Security Consultant and IT Auditor at SBS CyberSecurity (SBS), a company dedicated to helping organizations identify and understand cybersecurity risks to make more informed and proactive security decisions. She also serves as the Information Security Officer (ISO) for the company.

Laura maintains her Certified Information Systems Auditor (CISA), Certified Information Systems Manager (CISM), and Certified Data Privacy Security Engineer (CDPSE) certifications. She received her Bachelor of Science in Business Administration from the University of Tennessee at Chattanooga and is a graduate of the Southeastern School of Banking.

Laura has been involved in the financial services industry since 1993, serving in a variety of roles, including Information Security Officer, Internal Auditor, and Deposit and Loan Operations Manager. She joined the SBS team in 2015 with an extensive background in information security practices in banking.

Laura is passionate about helping organizations identify and understand cybersecurity risks, allowing them to make better, more informed business decisions. She is excited about sharing her knowledge through speaking engagements, webinars, and trainings. Laura is also a blog author with multiple articles published.

Learn more about Laura by connecting on LinkedIn.

QUICK FACTS

- Joined SBS in 2015 with an extensive background in banking.
- SBS Institute Instructor
- Has working experience in consulting and auditing and currently holds SBS' ISO role.
- Graduated from the Southeastern School of Banking.
- Holds a bachelor's degree and CISA, CISM, and CDPSE certifications.

TOPICS

These session topics represent only a sampling of the topics available (sessions descriptions available). SBS Institute will customize a topic that is perfect for your audience.

- 10 Cybersecurity Questions for Executives and Directors
- Cybersecurity 101 for Boards – What Directors Need to Know
- Building An IT Strategic Plan That Helps You Make Decisions
- Don't Buy a Data Breach: Cybersecurity Considerations During M&A
- Cybersecurity Mindset – How to Move from Reactive to Proactive
- Creating a Culture of Cybersecurity at Your Institution
- The Future of Cybersecurity: Trends You Should Know and Monitor (Threats and Controls)
- Reporting Critical Information Security Areas Upstream
- Responsibilities of the Information Security Officer
- Two Sides of The Same Coin: How and Why IT should be separated from IS
- You Are A Technology Company
- Cybersecurity Governance 101: How Any Business Can Start Building a Cybersecurity Program
- Securing Microsoft 365 – A Roadmap
- Phishing 101: How Employees Are Targets
- Modern Cyber Attacks Are Automated
- Today's Ransomware Threat – Don't Lose Your Data (And Your Business)
- Who's In Your Wallet?
- Online Reconnaissance – What the Internet Knows About Your Business
- Anatomy of an Attack – Ransomware
- Anatomy of an Attack – Business Email Compromise (BEC)
- Cyber Regulatory Compliance in 2023 – What Do You Need to Know?
- The Top 10 IT Audit Recommendations from 2022
- Components of a Strong Information Security Program
- FTC Safeguards Rule 2023: What Your Business Needs to Know
- Use Your Risk Assessment(s) To Make Better Cybersecurity Decisions
- How To Test (Audit) Your People, Processes, and Technology In 2023
- Vendor Management 2023 - How to Make Better Vendor Management Decisions
- SSAE18, SOC 1, SOC 2 - What Do I Need?
- What to Do When Your Vendor Gets Hacked
- 2023 Contract Review Checklist: What Is Your Contract Missing that Could Cost You?
- Managing Your Managed Service Provider – 12 Questions to Ask Your MSP
- 4 Steps to a Practical Business Continuity Plan
- What Goes into a Valuable Business Impact Analysis (BIA)?
- Where's Your Data? Using Your BIA and Data Flow Diagrams to Understand Risk
- Components of a Valuable Incident Response Plan
- How To Build Out an Incident Response Playbook
- We've Been Breached – Now What?
- How did that Data Breach Get Here? What You Need to Know about Digital Forensics
- Security Awareness Training – Best Practices for Keeping Your Employees Engaged
- Testing Your Technology – What Components of Your Technology Should You Audit?
- Assumed-Breach Testing: Why You Should Test as if a Hacker was Already in Your Network
- Your Reliance on Web Applications – Security Considerations for Critical Web Apps
- The Top 6 Controls to Reduce Your Risk of a Cyber Incident
- Remote Work is Here to Stay – Secure Your Devices and Information from Anywhere
- The Mythology of the Cloud – Considerations for Security Your Cloud Info
- Vulnerabilities in Data Center Hosting – Security Concerns to Address

TOPIC DESCRIPTIONS

10 Cybersecurity Questions for Executives and Directors

CEOs, senior management and Board members have historically struggled to understand the components of an Information Security Program, current security threats, and technology risks. Regardless, this group is ultimately responsible for the security of the organization's information, setting expectations or providing direction to management, and approving investments into cybersecurity. This discussion will review FFIEC Cybersecurity expectations, current threats to financial institutions, and touch on 10 questions that executives and board members must know to protect the bank in today's cybersecurity world.

Cybersecurity 101 for Boards – What Directors Need to Know

Many Board of Directors (BOD) members do not fully understand their bank's Information Security Program and cybersecurity threats facing them. Recent FFIEC guidance and publications have highlighted this issue. However, the Board is ultimately responsible for the security of their institution's information, setting the Bank's risk appetite, overseeing cybersecurity threats and risks, and approving financial investments into cybersecurity. The big question becomes: How does the Board become better equipped to make cybersecurity decisions?

This discussion will walk you through what exactly Directors and Senior Managers need to know about the their cybersecurity responsibilities. Topics include: current cybersecurity threats, FFIEC/OCC/FDIC/FRB regulatory guidance, FFIEC Cybersecurity Assessment Tool (CAT), including the Inherent Risk and Cybersecurity Maturity components, setting Cybersecurity Maturity goals, understanding Inherent Risk vs. Cybersecurity Maturity levels, and the different types of Risk Assessments at your institution (and how to leverage risk assessment results to make decisions). This session will enable you to make a difference as a Director at your financial institution and address the increasing regulatory expectations.

Building an IT Strategic Plan that Helps You Make Decisions

Does your IT Strategic Plan work for you, or is it just a document that you review once a year? Traditional FFIEC regulatory guidance calls for an IT Strategic Plan that identifies medium-to-long-term goals and allocations of IT resources over a three-to-five-year timeframe.

But how does your IT Strategic Plan help you to make decisions about which types of technology you WANT to deploy and WHO your institution wants to be when it comes to deploying technology?

This presentation will cover the following areas/topics:

- FFIEC Guidance on IT Strategic Planning
- The Law of Diffusion of Innovation
- What Kind of Bank Are You?
- What's Your Acceptable Level(s) of Risk?
- Lining Up Risk with Strategy
- Creating an IT Strategic Plan that can be your "North Star"

Don't Buy a Breach: Cybersecurity Considerations During M&A

The rising costs of digital transformation and cybersecurity protection have led to significant mergers and acquisitions over the last few years. As many smaller organizations that have not kept up with the tech needed to serve their customers are being acquired, it's important to note that these businesses likely didn't keep up with security either.

The last thing your organization wants to do is buy a data breach. Marriott would tell you it's not a walk in the park. This presentation will cover the things you need to know and questions that must be asked before closing a deal when acquiring another organization in today's cyber-world.

Cybersecurity Mindset – How to Move from Reactive to Proactive

The responsibility for managing and overseeing any organization today is massive and has evolved greatly over the last ten years to include investments in technology and cybersecurity. The Board of Directors and Senior Management are held accountable to the organization's shareholders, employees, customers, the community they serve, and (in many cases) regulators.

However, while more organizations work hard to be proactive with finances and operations, oversight of technology and cybersecurity tends to yet be very reactive. Funding and resources are typically very limited until an incident occurs that jeopardizes the operations of the business.

This presentation will cover the benefits of moving from a reactive to proactive cybersecurity mindset, including:

- Differences between a reactive and proactive cybersecurity mindset
- Results of a proactive cybersecurity mindset
- Tactical advice for being proactive
- Creating a culture of cybersecurity

Creating a Culture of Cybersecurity at Your Institution

The human element of information security is an increasing target for cybercriminals and generally considered the weakest area in information security. Security awareness and training on proper security protocols is an essential element of a strong cybersecurity program and regulatory compliance, but moving from reactive training to proactive training is the hard part.

We will discuss many methods of constructing an adequate security awareness and training program for both employees of your organization and customers of your online products and services, including awareness to cybersecurity issues, training on what is expected, and clear accountability for employees and management responsible for protecting customer information. These elements can help establish a lasting culture that includes a passion for protecting customer information and a desire to be successful against cybercrime.

In this session, we'll break down some of best practices to follow when providing training to employees and building a culture of cybersecurity, including:

- People, Process, and Technology
- Why People break rules
- Training topics and tactics
- Accountability for Security Awareness Training tests
- Building a Culture of Cybersecurity

The Future of Cybersecurity: Trends You Should Know and Monitor

The world of technology is very different today than it was just 5 years ago. From the technologies we use (cloud computing) to the threats we face (Ransomware, BEC) to the way we protect our data (MFA, Zero Trust), the cybersecurity landscape continues to evolve rapidly. It's highly likely that we'll look back 5 years from now and talk about how different our technologies and protections are today compared to back then.

In this session, we'll discuss the continued evolution and trends in cybersecurity we believe are likely to occur in the next few years, including:

- Cloud Computing Adoption
- Continued reliance on Vendors (Vendor Management)
- Machine Learning and Artificial Intelligence
- Advanced Cybersecurity Controls (Zero Trust, Behavioral Analytics, Automation, Threat Hunting)
- Future/Evolving Threats
- Customer Adoption of Technologies

Reporting Critical Information Security Areas Upstream

One of the most critical aspects of any Information Security Program is communication and sharing information. This is especially true with Executives and Board of Directors, who need to be educated and informed on all aspects of information security so they can ask better questions and make appropriate decisions. If the top level of the organization better understands the risks and the impact potential, it will help build a stronger information security culture throughout the organization.

So, what do you need to report upstream to help the Board and Executives understand your ISP and cyber risk? Let's dive in. This presentation will cover the following areas/topics:

- Regulatory Requirements for reporting ISP info upstream
- A Framework for Asking Better Questions
- What is most important to report upstream?
- How often should you report upstream?
- Setting a Culture of Security starts at the top

Responsibilities of the Information Security Officer

Being an Information Security Officer (or similar role) is a big responsibility in today's world of cyber threats and data breaches. This presentation is for those who are new to the ISO (or similar) role or have been the ISO for some time but want to review what is expected and how to be successful. As the ISO, part of your responsibility is building and maintaining the Information Security Program.

While an ISP has many important elements, there are 3 fundamental components: Risk Assessment(s), ISP Policies and Procedures, and Audit. The Risk Assessment will help you make decisions, the Policies and Procedures document the decisions for your institution to implement, and Audit verifies that those decisions have been properly implemented and are adequate controls to protect your institution.

This presentation will cover the following areas/topics:

- FFIEC Roles and Responsibilities of the ISP
- Building a strong Cybersecurity Culture
- Board Reporting
- Educational and Certification Paths
- Strong Risk Assessment Methodology
- Creating your ISP with Policies and Procedures

Two Sides of the Same Coin: How and Why IT Should be Separated from IS

Security versus Convenience is the battle that every organization faces when leveraging technology today. If you lean too heavily on Security, performing routine business functions may become inefficient and frustrating. If you lean too heavily on Convenience, you risk exposing your network and data to hackers. To make matters worse, you need to have a separation between IT Operations (who is managing your technology) and Information Security (IS) Operations (who is making sure you are secure).

The goals of IT are primarily efficiency and convenience. The goals of IS are primarily protection and security. The two functions are on the opposite end of the spectrum from one another, yet, the two must work together in harmony to meet your business objectives. In this session, we'll discuss:

- Differences between IT and IS
- Why IT Needs to be Separated from IS
- Who is Responsible for What?
- How IT and IS Can Work in Harmony

TOPIC DESCRIPTIONS

You Are A Technology Company

As your organization is reviewing its strategic plans, take a moment to evaluate the use of technology as a core component of your business. If most of you are being honest with yourselves you will realize that your organization has shifted from performing a service for a customer and using technology to make that service more convenient to truly operating as a technology company that offers your customer a specific service.

Look at it this way: if the majority of your customer interactions involve some component of technology, whether it's through online banking, mobile payments, other mobile applications, email, your internet-based telephones (VoIP), looking up customer information in your CRM or other software, you are a technology company.

In this session, we will discuss the following:

- Embracing Your Technology Company Status
- Changing Your View of Cybersecurity
- Acting Like a Technology Company

Cybersecurity Governance 101: How Any Business Can Start Building a Cybersecurity Program

Cybersecurity should be top-of-mind for any business today that relies on technology and the internet to do business. Cyber attacks affect businesses every 39 seconds. Understanding how cyber attacks occur and how to prevent, detect, and respond to such attacks is an important as ever.

But where do you start? Building a Cybersecurity Program for your business may seem like a monumental task, but in this session, we'll break it down into a few basic components that everyone can understand and implement, including:

- The Basic Components of a Cybersecurity Program
- Cybersecurity Standards and Best Practices Today
- What does Cybersecurity Governance include?
- How do I assess my Cyber Risk?
- Implementing Cybersecurity Decisions
- Testing your Cybersecurity Program

Securing Office 365 – A Roadmap

Office 365 is now utilized by over 650,000 companies and boasts more than 258 million users globally. 61% of Office 365 organizations are small businesses. Microsoft Office has long been a staple of the business world, but as we shift from hosting our data on-premise to the cloud, both the risks and rewards have changed.

One thing is for sure, your software is only as good as the security controls you implement to protect your organization. While Office 365 introduces new and unique threats, new and innovative controls are also a strong benefit of this cloud-based productivity suite.

This presentation will cover:

- An overview of Office 365 and components
- Threats to Office 365 and your organization
- Security Controls to consider deploying in Office 365, including Securing User Accounts, Logging/Monitoring, Threat Management, Alert Policies, Conditional Access, and more
- Testing your Office 365 implementation

TOPIC DESCRIPTIONS

Phishing 101: How Employees Are Targets

More than 80% of all cybersecurity incidents can still be traced back to the same root-cause: phishing emails.. Phishing campaigns are nearly fully automated and distributed as a service "crime-as-a-service." Phishing remains the most effective and cost-efficient attack vector from a cybercrime perspective. Considering the high probability of people falling victim to the destruction phishing can cause, phishing is truly a digital weapon of mass destruction.

This discussion will highlight the advancements in cybercrime and social engineering that targeting our most impactful, front-line resource: our people. Best practices will be discussed around improving perhaps the most vulnerable part of our businesses. With a reliable process, we can measure the level of risk and implement effective risk mitigating controls.

This presentation will cover the following areas/topics:

- Trends in Cyber Security Attacks
- Social Engineering and the latest phishing scams
- Logical controls to reduce risk around people
- Creating positive cybersecurity culture
- Testing your People

Modern Cyber Attacks are Automated

Many organizations make the mistake of thinking that most cyberattacks are "targeted" attacks against large businesses or high-value targets. In today's environment, nothing could be further from the truth.

Today's "hacker" doesn't look like the mental image of a hacker that most people imagine. It's not some 15-year-old kid in his (or her) mom's basement, drinking a liter of soda, eating a bowl of Cheetos, wearing a hoodie, and "hacking the planet." Today's hacker is a professional (in nearly every sense) that gets paid (well) to do a job (just like you).

This session will cover:

- How automation works in today's cyber attacks
- Know what you need to protect (information and assets)
- Top controls to mitigate cyber-attack risk
- What should you be testing in 2023 to properly protect your organization?

Today's Ransomware Threat – Don't Lose Your Data (And Your Business)

As you can see from watching the news, ransomware trends continue to rise. Ransomware was a $20 BILLION industry in 2023 and projects to exceed $265 BILLION by 2031. The average ransom demand continues to increase, as do the number of organizations being targeted, with no signs of slowing down.

Join us to recap the statistics related to ransomware and learn how to prepare for this growing threat. Numerous published best practices will be reviewed to assist our organizations to build stronger defenses. We'll also reflect on lessons learned from case studies captured from real-world ransomware cases has worked through.

In this session, we will cover the following topics:

- Ransomware Trends
- How Ransomware Infections Begin Today
- Top Controls to Mitigate Risk and Lessons Learned
- Regulatory Guidance and Expectations
- Ransom Payment and Recovery Methods

TOPIC DESCRIPTIONS

WHO's in Your Wallet?

Cybersecurity continues to increase its impact on financial institutions. Major (and minor) cyber incidents that continue to hit financial institutions, as we saw with First American Financial Corporation, Capital One, SolarWinds/Kaseya, and Block (formerly Square – mobile payments), remind us of the risks in our industry.

In this session, we will review the top cybersecurity threats facing financial institutions and review case studies to pull out essential lessons learned. This information will provide you with a solid foundation for making more informed decisions in providing oversight and direction for your institution. We will also review the cybersecurity responsibilities of the Board and provide a list of activities that can be used to increase involvement in information security. New legal precedents are being set that increase the liability for Directors of financial institutions.

Online Reconnaissance – Know What the Internet Knows About Your Business

If you've ever Googled yourself, you know there's plenty of information publicly available about each person via the Internet at all times. It's next to impossible not to leave a digital trail OR delete yourself from the Internet these days. The same can be said for your business. What information about your organization, employees, customers, vendors, and software is available via internet search tools? And even worse yet, how can cyber attackers leverage this information to build a specific, target attack against your organization or customers?

Open Source Intelligence (OSINT) is a common method hackers use to perform reconnaissance and create detailed, specific attack scenarios based on your organization. Odds are, a few searches or free tools can dig up more business information that you might initially think is readily available. The more tailored a cybercriminal can make their attack, the better chances they have at compromising your business.

This session will cover the types of information available to anyone on the internet, including:

- The OSINT model
- Online Cyber Risk Scores
- How to assess your internet-facing vulnerabilities
- Other freely available "hacker tools"
- How to reduce your attack vectors
- Accepting the risk when necessary
- Monitoring for reconnaissance

Anatomy of an Attack – Ransomware

Nearly every ISO and IT Manager's greatest fear is getting THAT phone call - the one where a user says they have a ransom note popping up on their screen. This is one of our greatest fears as well, but with a different spin - getting THAT phone call from a client. Unfortunately, we've been in this situation before and helped numerous organizations recover from ransomware.

In this session, we'll review two different ransomware attack scenarios from two different organizations that got different results while dealing with the aftermath of the attack - and WHY. We'll cover:

- Current Ransomware Stats and Tactics
- Typical Ransomware Attack Scenario Walk-Through
- Ransomware Case Study #1 and #2
- Differences and Results
- Top Controls to Mitigate Ransomware Risk

TOPIC DESCRIPTIONS

Anatomy of an Attack – Business Email Compromise (BEC)

According to recent studies, the average user has approximately 100 passwords to remember. With so many passwords to remember and a never-ending list of password requirements, it's no wonder so many people are reusing passwords. Unfortunately, we've seen many organizations have their business email accounts compromised through credential reuse. Business Email Compromise (BEC) can lead to not only propagating further BEC attacks, but also a full-blown data breach and network compromise. In this session, we'll walk through a real-world case study of a BEC attack, how BEC can turn into full network compromise, and lessons you can leverage to prevent this attack from occurring at your organization. We'll cover:

- The Scenario - What Happened?
- Typical BEC Attack Scenario Walk-Through
- How BEC Can Turn Into Full Network Compromise
- What's in Your Email?
- Top Controls to Mitigate BEC Risk

Cyber Regulatory Compliance in 2023 – What Do You Need to Know?

Since the Gramm-Leach-Bliley Act was passed in November of 1999, financial institutions in the US have been required to build and manage an Information Security Program, based on a risk assessment, that ensures the safety of confidential customer information.

A lot has changed since 1999, particularly in the world of cybersecurity, and regulatory agencies (FFIEC, FDIC, OCC, and the FRB) have released and updated many different standards around banking information security.

In this session, we'll cover the most important and impactful Cyber Regulatory Compliance standards to which financial institutions must adhere, including:

- FFIEC Guidance, such as the IT Management Booklet, IS Booklet, BCM Booklet, Outsourcing of Technology Services, the CAT, and the new Architecture, Infrastructure, and Operations (AIO) Booklet
- FDIC Guidance, such as FIL 44-2008 (Third Party Risk), InTREx, and additional threat-based guidance (Vulnerabilities, Cloud Computing, Malware, Technology Service Provider Contracts)
- OCC Guidance, such as Cyber-Related Sanctions, Bulletin 2013-29 (Third Party Relationships), Cyber Extortion and Destructive Malware, ATM Attacks
- Federal Reserve, such as SR 13-16 (Managing Outsourcing Risk) and Internet Banking Authentication

The Top 10 IT Audit Recommendations from 2022

Documenting an Information Security Program (ISP) is an important step in protecting your organization from cyber threats, but it's only as good as controls that are actually implemented. Testing your controls to ensure you're doing what you say you're doing – and what your doing is adequate – is the cornerstone to a strong ISP. The objective of a good IT Audit is to find areas of cybersecurity improvement for your organization.

SBS conducts over 500 audits per year across the US (primarily for financial institutions, but also includes businesses of all shapes, sizes, and industries). In this session, we'll share the 10 most-frequently recommended IT Audit findings over the past year, and how your organization can leverage these findings to get ahead of your next IT Audit.

Components of a Strong Information Security Program

Since the Gramm-Leach-Bliley Act was passed in November of 1999, financial institutions in the US have been required to build and manage an Information Security Program (ISP), based on a risk assessment, that ensures the safety of confidential customer information.

ISPs have evolved a bit over the last 20 years, however. Some of the biggest questions we hear about an ISP include: What are the major components of a modern ISP? What's the most effective way for an ISP to be structured? How does the ISP flow together? Let's discuss. This presentation will cover the following areas/topics:

FTC Safeguards Rule: What Your Business Needs to Know

Following the passing of the Gramm-Leach-Bliley Act in November of 1999, the FTC created the Safeguards Rule to ensure non-bank "financial institutions" – i.e., businesses that engage in activity that is "financial in nature" – are protecting their confidential customer information. The Safeguards Rule applies to auto dealerships the offer financing, real estate appraisers, check printing/cashing businesses, mortgage brokers, investment advisors, and more.

In December 2021, the FTC updated the Safeguards Rule to keep pace with current technology and modern threats. The new Safeguards Rule makes deploying MFA, implementing encryption, documenting an Incident Response Plan, and more a legal requirement for many businesses.

In this session, we'll cover:

- Is your business a "financial institution"?
- 2021 Safeguards Rule Updates – What's New and Important
- Timeframes for implementation
- And more!

Use Your Risk Assessment(s) to Make Better Cybersecurity Decisions

As financial institutions, you're required to perform numerous risk assessments throughout the Information Security Program lifecycle: IT, Vendor, Business Process (BIA), and Cybersecurity risk assessments. Each serve a different function and goal, but one thing remains constant – if your risk assessment isn't helping you to make decisions, it's not a good risk assessment.

So how do you build a risk assessment that helps you to make better decisions? Let's discuss.

This presentation will cover the following areas/topics:

- Regulatory Requirements of ISP Risk Assessments
- Differences in the different types or Risk Assessments
- A framework for valuable risk assessments
- Make decisions from your IT Risk Assessment, Vendor Risk Assessment, BIA, and Cybersecurity Risk Assessment
- How do these risk assessments work together?

How to Test (Audit) Your People, Processes, and Technology in 2023

There are three (3) phases to creating an Information Security Program for any organization: 1) planning and preparation, 2) implementation, and 3) testing and verification. When it comes to testing your ISP, one of the big questions you should ask – both of yourself and your auditor(s) – is "where does our risk really live?" Are you testing your ISP because you have to, or are you testing your ISP because you really want to protect your organization and your customer's data from a cyber attack?

This presentation will cover the following areas/topics:

- People, Process, and Technology
- Minimum Requirements for Testing Your ISP
- Best Practices for Testing Your ISP
- Reactive Testing vs. Proactive Testing
- Additional Security Testing to Consider

Vendor Management 2023 - How to Make Better Vendor Management Decisions

The fundamentals of compliance-based Vendor Management have been around since 2004's FFIEC Outsourcing of Technology Services booklet was released. While VM has evolved a bit over the years, the process is essentially still the same. We gather documentation, review it, and try to make a decision whether we keep doing business with this company or not. Analyzing vendor documentation is important, but the real question we need to ask is this: how do we understand if our vendors are really protecting your data?

This presentation will cover the following areas/topics:

- Regulatory Vendor Management Guidance over the years
- How to build a "modern" Vendor Management Program
- Other ways to manage Vendor Risk
- Other tools to review Vendor security
- Supply Chain Management/4th Party Management

SSAE18, SOC 1, SOC 2 - What Do I Need?

All regulators say, in a similar fashion, that we must understand the security controls of a third party "to the same extent" as we understand our own internal controls. Most industries rely heavily on SSAE18 Audit Reports, and the Service Organization Control (SOC) 2 reports provided by vendors. What are the differences between these different reports, and which should we be requesting? And once we obtain them, how do we understand the security controls to the "same extent" as our own?

We will explore the different types of SOC reports provided by vendors and highlight the best items that should be requested from vendors. In addition to what report(s) to ask for, we will explore different SOC report types in detail to highlight what to look for – and why. The following items will be addressed in this discussion:

- Vendor Management Regulatory Expectations
- Third Party (Vendor) Management best practices
- Fourth Party/Supply Chain Management
- Required Documentation, including the different SOC Report types
- Other items useful in Vendor reviews
- Detailed Due Diligence and Contract Review questions

What to Do When Your Vendor Gets Hacked

In today's world, nearly every business function can be outsourced to a cloud provider. However, outsourcing a business function does not outsource the risk of protecting your customer information. Proactive vendor management is essential for organizations to make the right business decisions about the partners they choose. Combining Vendor Management with a strong Incident Response Plan helps prepare your organization for the possibility of a vendor breach.

In this session, learn tips on how to respond if a vendor is compromised, and how identifying and understanding cybersecurity risk gives your organization a competitive advantage in a digital world. Highlights include:

- Key components to modern vendor management
- The must haves of Vendor Management + Incident Response
- The role digital forensics plays in a vendor breach
- Insurance and legal
- Controls to prevent a network compromise
- What to test, including vendors

2023 Contract Review Checklist: What Is Your Contract Missing That Could Cost You?

Ah, vendor contracts – perhaps the bane of every Vendor Manager's duties. Some contracts are new, but others are 10+ years old. Some contracts are well-written, but many contracts are from a time when cybersecurity and incident notification requirements were not like they are today.

So, what should you do about the myriad of different contracts you have with all your vendors? If that's your burning question, you're in luck – this topic is just for you!

In this session, we'll discuss the key components of reviewing vendor contracts, including:

- Regulatory Guidance on Contract Reviews
- Types of Contracts
- Creating Contract Review Question Sets
- How to Handle Missing, Critical Contract Elements
- How Often Should You Review Contracts?

Managing Your Managed Service Provider – 12 Questions to Ask Your MSP

Many organizations leverage a Managed Service Provider (MSP) to manage their IT infrastructure, often providing more expertise while saving some cost. But when it comes to protecting data, the term "cybersecurity" can mean different things to different organizations. The goals of Information Technology (convenience and availability) far different than the goals of Information Security (protection and loss prevention).

This session will cover the gamut of areas to consider, including:

- Information Technology vs. Information Security
- Types of Managed Services Providers
- Traditional Vendor Management of MSPs
- Modern Vendor Management of MSPs
- Characteristics of a Good MSP Partnership
- Questions to ask before hiring an MSP

4 Steps to a Practical Business Continuity Management Plan

Federal regulators require institutions to maintain Emergency Preparedness Plans, such as Business Continuity, Disaster Recovery, and Pandemic Preparedness. These plans ensure continuity of the institution in an unlikely event a significant incident or disaster occurs. The consequences to a financial institution can be severe if proper disaster recovery and business continuity planning does not occur and continuity of business fails. In fact, many significant business continuity risks are connected directly to disasters originating from cybersecurity threats.

Building a valuable, comprehensive Business Continuity Management (BCM) Plan is no small task, and the Plan must take a holistic view of the institution and involve representation from all functional units of the organization. So, where do you start, and how to you build a BCMP that will be valuable to the institution?

In this session, we'll highlight how to build a BCMP in 4 steps:

- Start with your Risk Assessment – the Business Impact Analysis
- Build your Business Continuity Management Plan documentation
- Test your BCMP via Tabletop Walkthroughs to improve your processes
- Functional Business Continuity/Disaster Recover Testing to ensure your recoverability

What Goes into a Valuable Business Impact Analysis?

It is no secret that a Business Continuity Management Plan (BCMP) is an important document to have in your arsenal, especially when responding to events (such as natural disasters or cyberattacks) that may interrupt or halt business operations. As with other critical areas of Information Security, to build a valuable BCMP, you need to start with a risk assessment. In the case of BCMP, that risk assessment is called a Business Impact Analysis (BIA).

A good BIA helps you to make important recovery decisions, specifically which business processes should you restore first (and in what order), and what is needed to restore those business processes. So how do you build such a valuable BIA?

This presentation will cover the following areas/topics:

- Regulatory Requirements of BCP and BIA
- Components of a valuable BIA
    - Impacts
    - Timeframes
    - Dependencies
- Creating a Recovery Priority Rating for Business Processes
- Using your BIA to drive your BCP

Using Your BIA and Data Flow Diagrams to Understand Risk

Data Flow Diagrams (DFDs) are one of the areas financial institutions tend to struggle with quite often. When performed as a compliance exercise (DFD's are the top FFIEC CAT control that institutions aren't completing), a DFD often looks like a Network Diagram and has little value.

But when we dive in and look at building a valuable DFD, you'll find an answer to the question "where does my data go when it leaves my network, and how is that data being protected?"

This presentation will cover the following areas/topics:

- Regulatory Guidance on Data Flow Diagrams
- How do you get real value from a DFD?
- Starting with your Business Impact Analysis
- How to build a Data Flow Diagram that has value
- Using your BIA and DFDs to understand your risk

Components of a Valuable Incident Response Plan

In today's cybersecurity world, we can't afford to assume that our business will never be compromised. Organizations must properly invest in cybersecurity - not only in preventing cyber attacks, but also in the ability to detect and response to today's cyber threats. With cyber attacks on the rise, it's time to sharpen your response procedures and improve your Incident Response Plan (IRP).

In this session, the core steps required for most cyber incidents will be highlighted, and specialized components for malware, ransomware, BEC, DDoS, and network compromise incidents will be examined. Explore the importance of incorporating digital forensic analysis procedures into your IRP to better address emerging threats and decrease cyber risk.

In this session, we'll discuss the following components of an Incident Response Plan that all organizations should consider:

- Roles and Responsibilities
- Threat Assessments/Indicators of Compromise
- Incident Containment, Eradication, and Recovery Playbooks
- Internal and External Communications
- Integration of Forensics
- Notification Requirements
- And more!

How to Build Out an Incident Response Playbook

The thing about Incident Response, just like Business Continuity (and insurance), is that we all hope the scenarios we know can happen never actually occur. However, the point of planning is to anticipate the bad things happening and have a plan to deal with those incidents, should they occur.

While can be difficult to document a response for Incident Response scenarios that have never occurred, building out step-by-step scenarios into an Incident Response Playbook might just save your organization time, money, resources, or even the business itself is something bad does happen. How do you create your own Incident Response Playbook?

This presentation will cover the following areas/topics:

- Regulatory requirements of an Incident Response Plan (IRP)
- Components of a valuable IRP
- What is an Incident Response Playbook?
- Testing Your Incident Response Playbook
- Using Your Playbook to improve your IRP

How did that Data Breach Get Here? What You Need to Know about Digital Forensics

Prevention tends to be our primary focus in protecting our organizations, but how would we know if we failed to prevent an attack? Knowing what cyber threats are realistic for your business and how to detect those threats is a challenging task. Today's statistics show it takes more than 200 days to detect a breach on average, suggesting we don't fully understand how realistic cyber threats are to our organizations or how to detect such threats.

Digital Forensics is the scientific method of identifying, extracting, documenting, and preserving computer evidence – most commonly used to determine the cause (and results) of a computer security incident on a device or network. A Digital Forensics investigation is often required to determine the full extend on an incident – but many organizations are not properly prepared for a successful investigation.

In this session, we'll discuss everything you need to know about Digital Forensics, including:

- Types of Digital Forensics
- Components of a Digital Forensics Investigation
- Digital Forensic and Incident Response Preparation
- Digital Forensics Skills and Tools

How did that Data Breach Get Here? What You Need to Know about Digital Forensics

Prevention tends to be our primary focus in protecting our organizations, but how would we know if we failed to prevent an attack? Knowing what cyber threats are realistic for your business and how to detect those threats is a challenging task. Today's statistics show it takes more than 200 days to detect a breach on average, suggesting we don't fully understand how realistic cyber threats are to our organizations or how to detect such threats.

Digital Forensics is the scientific method of identifying, extracting, documenting, and preserving computer evidence – most commonly used to determine the cause (and results) of a computer security incident on a device or network. A Digital Forensics investigation is often required to determine the full extend on an incident – but many organizations are not properly prepared for a successful investigation.

In this session, we'll discuss everything you need to know about Digital Forensics, including:

- Types of Digital Forensics
- Components of a Digital Forensics Investigation
- Digital Forensic and Incident Response Preparation
- Digital Forensics Skills and Tools

Security Awareness Training – Best Practices for Keeping Your Employees Engaged

It's time to shift our thinking when it comes to security awareness training. Yearly education and testing just doesn't cut it in today's cyber world. Security awareness is a topic we should have in front of our people on a much more consistent basis.

However, as we all know, creating an engaging Security Awareness Training program is more than words or flipping a switch – it involves thoughtful and deliberate action across the organization, as well as accountability for building a culture of cybersecurity. Culture changes and engagement also has to start at the TOP of the organization, or it will be meaningless downstream.

Join us for this session on creating a Security Awareness Program that keeps people engaged, including:

- Cyber Threat's New Normal
- People, Process, and Technology – which is the weakest link?
- Compliance-based vs. Proactive Security Awareness Training
- Building an Effective Security Awareness Training Program (for all areas of your organization)
- Topical Training Ideas
- Why Accountability Matters Most

Testing Your Technology – What Components of Tech Should You Audit?

Testing your technology in 2023 is a critical component of ensuring your network, organization, and confidential information are protected against today's cyber threats. However, there are many different ways to test your technology and many different technologies to test. Where do you start, and where should you focus? This session will feature logical and physical tactics for testing your technology to highlight risk and better protect your institution and customers from cyber attacks.

We'll discuss the following ways to test your technology in 2023:

- Vulnerability Assessment
- Penetration Testing
- Firewall Configuration Review
- Web Application Testing
- Password Audit
- Remote Access Review
- Email System Review

Assumed-Breach Testing: Why You Should Test as if a Hacker was Already in Your Network

On average, it takes an organization 287 days to detect and contain a data breach. Hackers today are very good at breaking into networks and staying undetected for long periods of time before executing their ultimate objectives. When a cyber incident inevitably occurs, your best bet is to assume your network is compromised and act accordingly, rather than assume you're not compromised and carry on like normal.

One of the most important questions to ask yourself is: "If a hacker was in my network, would I know?" Testing your internal and external network security controls regularly is an important way to find the answer. But what happens if the Penetration Test has little or no success?

Assumed-Breach Testing simulates the initial foothold an attacker might obtain, allowing for more in-depth testing and provides a unique perspective of the organization's readiness for a real-world breach. Assumed-Breach Testing helps answer the question of "what can happen if we were breached?"

In this session, we'll discuss the different components and objectives of Assumed-Breach Testing, including:

- Modern Cyber Attack Vectors
- Identifying your data stores
- Lateral Movement and Persistence
- Privilege Escalation
- Data Exfiltration
- How to perform Assumed-Breach Testing
- And more!

Your Reliance on Web Applications – Security Considerations for Critical Web Apps

Gone are the days – thankfully – of having to download every individual software application on all servers or workstations (and update those apps regularly). In today's interconnected, cloud-based work environment, most of our critical work-related applications are hosted on the internet – accessible any time and from any location.

However, convenience often has a cost. Being able to access our apps online comes with additional risks. If you can see the application on the internet, so can a hacker.

Securing the web applications we use to do business, and thus our confidential information, has never been more important. In this session, we'll discuss the most important security considerations for your web apps, including:

- Inventory and Risk Assessment
- Multi-Factor Authentication (MFA)
- Access Controls and Passwords
- Encryption and Data Transmission
- Secure Code Reviews
- Web Application Penetration Testing
- Vendor Management

The Top 6 Controls to Reduce Your Risk of a Cyber Incident

Cyber attacks are CEOs #1 fear in 2022, according to PWC's annual CEO survey. If you read the news headlines regularly, one can understand why. However, a huge gap exists between most organization's cybersecurity capabilities and the fear of a data breach or ransomware.

So, what should your organization do to close the gap and reduce your cyber risk?

This session will discuss the Top 6 Controls your organization should be implementing to significantly reduce your risk of a cyber attack. We'll walk through some of the most probably cyber attack scenarios and demonstrate how these top controls can mitigate your cyber risk, as well as discuss some additional risk-mitigating options every organization should consider.

Remote Work is Here to Stay – Secure Your Devices and Information From Anywhere

If COVID-19 has taught us one thing, it's that today's workforce is and will continue to be more remote and mobile going forward than ever before. Many organizations have allowed remote working at historic levels, and many of these remote workers will not return to a physical office in the same capacity as pre-pandemic.

While remote working may trend back to in-office work after pandemic levels come down, many remote workers will stay remote. As organizations, we have to ensure the security of our business information, our employees, and our customers… regardless of whether someone's working from a corporate office or their home office.

This presentation will cover the following areas/topics:

- Remote working threats
- Must-have remote working governance (documentation)
- Top controls to mitigate remote working risk
- Remote worker training

The Mythology of the Cloud – Considerations for Security Your Cloud Info

Cloud computing can be an ambiguous term, but always remember: the "cloud" is really just your stuff on other people's computers. Modern cloud computing services have many advantages but also come with additional risks. Keep in mind, it's ultimately YOUR responsibility for protecting your customer information, no matter where it's stored.

In this session, we'll discuss modern cloud computing environments, controls to mitigate risk in cloud environments (from your organization's end and from the cloud provider), and what type of documentation to request from your cloud provider relating to cybersecurity testing and compliance.

Vulnerabilities in Data Center Hosting – Security Concerns to Address

Outsourcing parts, or even all, of your network has become a very common practice. In theory, having a data center host all or parts of your network is both a security upgrade (that's what they do, after all) and a cost saving measure. However, outsourcing your network certainly comes with its share of risk.

The bottom line is that it's your organization's responsibility to ensure the security of your information and devices, regardless of where that information or those devices are physically located. This responsibility includes making sure you have oversight and insight into how your information and devices are being managed – at all times - from a security perspective.

In this session, we'll discuss how to gain better insight into data centers that host information or devices for you, including:

- Data Center/Vendor Management Best Practices
- Supply Chain Risk
- The types of documentation you should be receiving
- How to review appropriate security documentation from vendors
- What do to about vendors that don't provide appropriate security documentation
- The Right to Audit
- Managing Acceptable Levels of Risk and Known Risk Exceptions

CYBERSECURITY SEMINAR
Overview

Program Summary

This seminar is designed to provide training on evolving cybersecurity threats and what your bank should do to build a strong Information Security Program that helps protect against these threats. We will identify components of a comprehensive Information Security Program that enables successful IT Examinations and minimizes your risk against real-world threats. This seminar will walk you through various FFIEC, FDIC, and OCC resources, as well as other industry best practices. We will also review some timely hot-stove topics, including Pandemic Preparedness, Managed Service Providers, and creating a Culture of Security at your institution.

Who Should Attend

This seminar is perfect for Information Security Officers and Information Technology Staff, but will also provide great value to Compliance Officers, Auditors, Presidents, and Board of Directors

Topics Covered

Day 1

- Modern Cyber Attacks are Automated
- Current Regulatory Guidance and GLBA Overview
- Use your IS Risk Assessments to make better decisions, including:
  - IT Risk Assessment
  - Vendor Management
  - Business Processes (BIA)
  - Cybersecurity (Organizational) Risk Assessment
- Responsibilities of an Information Security Officer

Day 2

- How to Build Out an Incident Response Playbook
- Real-World Case Study: Ransomware
- Real-World Case Study: Business Email Compromise
- Top 6 Controls to Mitigate Cyber Risk

1. Take away ideas to create and maintain a culture of cybersecurity at your organization.

2. Prepare for successful IT Examinations and minimizes your risk against real-world threats

3. Prepare to "fail well" with the building blocks of a modern Incident Response Plan for today's cyber threats

INCIDENT RESPONSE SEMINAR

Overview

Program Summary

In today's cybersecurity world, we can no longer hide behind the assumption that a business will never be compromised. It is not a question of **IF** a compromise will occur, but **WHEN** will it occur. When that incident occurs what should we, as technology professionals, do to minimize the attackers' intrusion and data theft? A cyber incident is no different than a physical bank robbery in terms of the seriousness of the crime. In a crime scene investigation, evidence would be preserved, and a thorough investigation would commence. All too often, we respond to cyber incidents with intentions to eradicate the issue and get the system back into production as fast as possible to avoid downtime. Such responses often mean not getting to the true root cause of the incident, which increases the likelihood for recurrence and additional downtime.

In reality, we need to ensure our Incident Response Plan helps us to answer some major questions. If you don't know the answer to these questions, you won't want to miss this seminar:

1. If it's not a matter of if, but when - are we **planning to fail well**?
2. If an unauthorized individual was in my network, would I be able to tell?
3. If someone was sending our data out the virtual backdoor, how would we know?
4. If we were robbed digitally, do we know what a good digital investigation looks like? Do we have someone that can help?

Who Should Attend

This seminar is perfect for Information Security Officers and Information Technology Staff, but will also provide great value to Compliance Officers, Auditors, Presidents, and Board of Directors.

Topics Covered

- The seemingly insurmountable threat of cybercrime
- Core steps necessary for various incident types
- Special emphasis on phishing, malware, CATO, and unauthorized access incidents
- The basics of knowing what "normal" on your network looks like how to identify "abnormal"
- Identifying your Key Risk Indicators
- Forensic analysis procedures to better collect and evaluate evidence
- If security measures fail, you will learn the how-to's of:
    - Internal Communications
    - Incident Containment, Eradication and Recovery
    - External Communications

1. Ensure your organization has successfully planned to fail well.

2. Understand how to minimize an attackers' intrusion and data theft.

3. Identify the most important questions your Incident Response Plan must answer.

BUSINESS CONTINUITY MANAGEMENT SEMINAR

Overview

Program Summary

Federal regulators require banks to maintain emergency preparedness plans, such as Business Continuity, Disaster Recovery, and Pandemic Preparedness. These plans ensure the continuity of the bank in the unlikely event of a significant incident or disaster occurring. The consequences to a financial institution can be severe if proper disaster recovery and business continuity planning does not occur and continuity of business fails. In fact, many significant business continuity risks are connected directly to disasters originating from cybersecurity threats. This one-day seminar will cover the essentials of what to include in a valuable, comprehensive Business Continuity Plan that helps minimize any potential downtime for your institution. We'll also highlight real case studies for hands-on practical application in your institution.

Who Should Attend

This seminar is perfect for Information Security Officers and Information Technology Staff, but will also provide great value to Compliance Officers, Auditors, Presidents, and Board of Directors.

Topics Covered

- Regulatory Requirements – Including the Updated FFIEC BCM Handbook
- Types of Incidents and Disaster Planning
- Business Impact Analysis
- Risk Assessment
- Plan Development
- Dusting off the Pandemic Preparedness Plan – What's it Good For?
- Testing and Improving the Plan
- Tying Business Continuity, Incident Response, and Vendor Management Together

1. Learn from real-world case studies.

2. Gain an understanding of how to build a valuable and comprehensive BCP.

3. Ensure your organization minimizes any potential downtime.

BUSINESS CONTINUITY AND INCIDENT RESPONSE SEMINAR

Overview

This seminar is similar to the individual Business Continuity Management and Incident Response Seminars, except the morning will be dedicated to Business Continuity, and the afternoon to Incident Response.

Program Summary

Federal regulators require banks to maintain emergency preparedness plans, such as Business Continuity, Disaster Recovery, Pandemic Preparedness, and Incident Response. These plans ensure the continuity of the bank in the unlikely event of a significant incident or disaster occurring. The consequences to a financial institution can be severe if proper disaster recovery, business continuity, and incident response planning does not occur and continuity of business fails. In fact, many significant business continuity risks are connected directly to disasters originating from cybersecurity threats. This one-day seminar will walk you through what should be included in a valuable, comprehensive Business Continuity and Incident Response Plans that helps minimize any potential downtime for your institution.

Who Should Attend

This seminar is perfect for Information Security Officers and Information Technology Staff, but will also provide great value to Compliance Officers, Auditors, Presidents, and Board of Directors.

Topics Covered

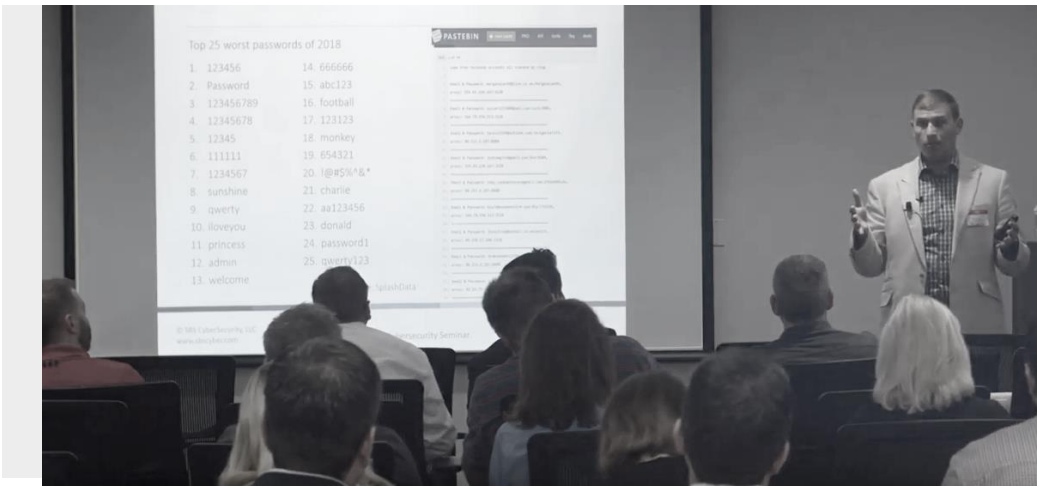
- Business Continuity Session
  - Regulatory Requirements – including the updated FFIEC BCM Handbook
  - Business Impact Analysis & Threat Assessment
  - What to include in your documented Business Continuity Plan
  - Testing and Improving the BCP
- Incident Response Session
  - Regulatory Requirements – including the FFIEC Information Security Handbook
  - Incident Identification & Threat Assessment
  - Key Risk Indicators
  - Incident Response Playbooks – how to handle specific incidents
  - Digital Forensics Basics
  - Testing and Improving the IRP
- Tying Business Continuity, Incident Response, and Vendor Management together

1. Be prepared to continue doing business with minimal downtime after an incident or disaster.

2. Gain an understanding of how to build a valuable and comprehensive BCP and IRP.

3. Learn how to tie business continuity, incident response, and vendor management together.

CERTIFICATIONS
Overview



ASSOCIATION VALUE

- Promotes other association education events (webinars, conference events, seminars): 4 hours annually of continuing education per certification
- 20% commission on all certification activity in your state
  - Certifications sales
  - Annual membership fee
  - Exam retakes and course extensions
- Highly valuable educational solution for your members
- Turn-key solution
  - Association markets the program
  - SBS handles registration and delivery
  - Always online - with options for onsite
- Low risk investment, no financial commitment from the association

STUDENT VALUE

- Gain confidence in your Risk Assessments and ISP and know they are valuable
- Demonstrate your expertise to auditors, and examiners, Senior Management, and the Board of Directors.
- Learn to perform essential cybersecurity functions efficiently and effectively
- Mature your cyber program by addressing real-world cybersecurity issues and establishing solutions
- Collaborate with a cybersecurity expert to build material to implement at your institution
- Be successful in a new information security role
- Invest in your cybersecurity knowledge and future

CERTIFICATIONS

Online and Onsite Offerings

Online vs Onsite Offerings

ONLINE CERTIFICATION

- 20% commission for all online certifications in your state
- Online, on demand delivery
- Self-paced
- Associations can help promote an online start date
- Allowed 10 weeks to complete
- 10 certification options
- Email and phone access to instructor

ONSITE CERTIFICATION

- 20% commission on your onsite certification
- SBS covers all speaker, meal, and facility costs and promotes the event through social and email marketing
- Association helps promote the event and handles logistics
- 2-day "boot camp" style sessions
- 4 certification options
  - Certified Banking Security Manager
  - Certified Banking Vendor Manager
  - Certified Banking Cybersecurity Manager
  - Certified Banking Security Technology Professional
- Allows for peer networking
- In-person collaboration with instructor

CERTIFICATIONS
Course Details

2023 Online Course Calendar

Course	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Certified Banking Security Manager		7th			2nd			1st			1st	
Certified Banking Security Technology Professional	3rd			4th			11th			3rd		
Certified Banking Vendor Manager			7th			6th			12th			5th
Certified Banking Incident Handler	10th			18th			18th			17th		
Certified Banking Ethical Hacker			14th			13th			19th			12th
Certified Banking Security Executive		14th			9th			8th			7th	
Certified Banking Vulnerability Assessor			28th			20th			27th			19th
Certified Banking Cybersecurity Manager		21st			16th			15th			14th	
Certified Banking Forensic Investigator		28th			23rd			22nd			28th	
Certified Banking Business Continuity Professional	24th			25th			25th			24th		

Courses Offered Online and Onsite

CERTIFIED BANKING SECURITY MANAGER (CBSE)

This course will assist you in maturing and managing your information security program to meet cybersecurity and regulatory expectations. The resources and exercises available with this course will help you develop valuable material to take back to your institution.

- ✓ Understand how to successfully implement and manage each component of your information security program.
- ✓ Access to a library of over 50 cybersecurity resources including FFIEC handbooks, best practice standards, example processes, and guidance.
- ✓ Boost your knowledge of layered security programs.
- ✓ Gain confidence in your decision making with comprehensive cybersecurity knowledge.

- Manager Path.

Who Should Attend: ISO, Auditor, IT Manager, Compliance, Security Officer, Operations Officer

CERTIFIED BANKING VENDOR MANAGER (CBVM)

This course will assist you in maturing and managing your information security program to meet cybersecurity and regulatory expectations. The resources and exercises available with this course will help you develop valuable material to take back to your institution.

- ✓ Understand how to successfully implement and manage each component of your information security program.

CERTIFIED BANKING CYBERSECURITY MANAGER (CBCM)

This course will focus specifically on each element of the FFIEC Cybersecurity Assessment Tool, including continual updates. In addition, we will complete detailed lab exercises that demonstrate how each process works.

BONUS! Students should be able to complete the actual assessment of their institution as part of the course.

- ✓ Complete the actual Cybersecurity Assessment for your institution.
- ✓ Develop a deeper understanding of commonly missed baseline controls.
- ✓ Build a solid foundation of understanding for the FFIEC guidance.
- ✓ Gain the knowledge to better defend against cybersecurity threats.
- ✓ Receive a comprehensive collection of cybersecurity resources.

Executive Path.
Who Should Attend: Director, President, CIO, CISO, CTO, CFO, COO

CERTIFIED BANKING SECURITY TECHNOLOGY PROFESSIONAL (CBSTP)

This course will allow you to explore the technical design and implementation of Information Security Program controls.

- ✓ Gain a better understanding of risk management, documentation, and auditing.
- ✓ Discuss real-world cybersecurity risks and review possible technical controls and security configurations.
- ✓ Complete hands-on exercises with a variety of security testing software, such as Kali Linux.
- ✓ Gain working experience with security tools, troubleshooting and analysis tools, vulnerability scanning, and patching processes.
- ✓ Reference security standards from NIST and CIS

Technical Path.
Who Should Attend: IT Manager, Network Administrator, IT Specialist

Courses Offered Online Only

CERTIFIED BANKING ETHICAL HACKER (CBEH)

This course will allow you to master the concepts and technologies used by today's hackers to better defend your institution.

- ✓ Gain real-world cybersecurity defense knowledge and skills you can put to use immediately.
- ✓ Take security into your own hands with the ability to run scanning processes on demand as threats arise.
- ✓ Better understand your risks so you can communicate them to your team more effectively.
- ✓ Assist with the Cybersecurity Controls domain of the FFIEC Cybersecurity Assessment.

Technical Path.

Who Should Attend: IT Manager, Network Administrator, IT Specialist

CERTIFIED BANKING INCIDENT HANDLER (CBIH)

This course will provide you with an increased understanding of the best practices related to handling common incidents in the banking industry and minimizing losses.

- Become an expert in responding to incidents and minimizing losses.
- Build out Incident Response procedures to take back to your institution.
- Assist with the Threat Intelligence and Collaboration as well as the Cyber Incident Management and Resilience domains of the FFIEC Cybersecurity Assessment.

Manager Path.

Who Should Attend: ISO, Auditor, IT Manager, Compliance, Security Officer, Operations Officer

CERTIFIED BANKING FORENSIC INVESTIGATOR (CBFI)

This course will provide you with an understanding of the fundamental digital forensic and incident response processes necessary to address the growing digital investigative needs of your institution.

- ✓ Understand why and how digital investigations are treated like a real criminal investigation.
- ✓ Know how to get the data you need to prosecute evil insiders and successfully defend against attackers.
- ✓ Create a proper chain of custody for digital incidents.
- ✓ Be prepared for incidents with detection, containment, and eradication.
- ✓ Assist with the Cybersecurity Controls and Cyber Incident Management and Resilience domains of the FFIEC Cybersecurity Assessment.an expert in responding to incidents and minimizing losses.

Technical Path.

Who Should Attend: IT Manager, Network Administrator, IT Specialist

CERTIFIED BANKING SECURITY EXECUTIVE (CBSE)

This course will provide you with a clear understanding of management requirements for Information Security and a strategic technology background for future planning.

- ✓ Gain a better understanding of the key elements of an Information Security Program.
- ✓ Make more informed decisions about risk mitigating activities.
- ✓ Be empowered to ask the right security questions.
- ✓ Design roles and responsibilities for effective cybersecurity governance.

Executive Path.

Who Should Attend: Director, President, CIO, CISO, CTO, CFO, COO

Commented [PH1]: Add CTP?

CERTIFIED BANKING BUSINESS CONTINUTIY PROFESSIONAL (CBBCP)

This course will use real-world exercises to help you build a useful and repeatable business continuity plan to take back to your institution.

- ✓ Develop a clear understanding of a business continuity plan, which will make your work more efficient and effective.
- ✓ Confidently implement and manage a strong business continuity plan.
- ✓ Generate new ideas and scenarios for business continuity testing.
- ✓ Prepare your institution for the worst-case scenario.
- ✓ Gain practical solutions for FFIEC Appendix J requirements.

Manager Path.

Who Should Attend: ISO, Auditor, IT Manager, Compliance, Security Officer, Operations Officer

CERTIFIED BANKING VULNERABILITY ASSESSOR (CBVA)

This course will guide you as you learn how to take security into your own hands with the ability to identify and remediate vulnerabilities at your institution.

- ✓ Gain a clear understanding of scanning tools available in the market.
- ✓ Explore best practices for continuous vulnerability monitoring.
- ✓ Find bugs to patch, security settings to fix, and software to remove on your systems.

Technical Path.

Who Should Attend: IT Manager, Network Administrator, IT Specialist

CONTACT SBS INSTITUTE

If you'd like additional information on the SBS Institute or how our educational offerings can help you, please contact us:

605-269-0909

sbsinstitute@sbscyber.com

www.sbscyber.com

SBS INSTITUTE