SBS INSTITUTE

Top Audit Recommendations

For 2025

Cody Delzer – Principal Consultant

Cody Delzer

- Principal Consultant
- CISA, CDPSE
- Bachelor's Computer & Network Security from Dakota State University
- Cody.Delzer@sbscyber.com
- 605-228-2829
- www.sbscyber.com

SBS Institute

- sbsinstitute@sbscyber.com
- 605-269-0909

What’s Changing?

- New/Updated Guidance and Regulation in 2024 and 2025.
  - **2024**
    - FFIEC Development, Acquisition, and Maintenance Booklet (updated August 2024)
    - NIST CSF 2.0 (April 2024)
    - FFIEC CAT Sunsetting effective August 2025
  - **2025**
    - AI/ML Risk Management Guidance – Confirmed; regulators issued model risk updates and governance expectations.
    - FFIEC CAT Sunset – Transition to NIST CSF 2.0, CISA CPGs, CRI Profile, CIS Controls.
    - Operational Resilience – FFIEC and OCC emphasize resilience and incident response maturity.
    - Cloud & API Security – Supervisory priorities now include governance and API risk.

SBS INSTITUTE

Top 10 Audit Recommendations

1. Log Management

CONTROL

- Does the Organization log network/domain events, such as successful logins and failed logins and Core Banking failed logins?
- Does the Organization log firewall events? Does internal staff or the managed service provider audit firewall activity on at least a quarterly basis?
- Has the Organization set alert parameters for detecting Information Security incidents prompting mitigating actions?
- Does the Organization review internet access, remote access, audit and security, and administrative activity logs?
- How does the Organization ensure secure storage of audit log records and other security event logs?

1. Log Management

OBSERVATION

- The Organization has not implemented procedures to regularly review logs or reports containing the following:
  - Web content filtering / Internet access monitoring
  - Failed logins (core banking, network)
  - Firewall events
  - Audit and security logs
  - Administrator activity (including independent review)
  - Vendor / Employee remote access
  - Problem logs (ticketing system)
- Audit log records and other security event logs are stored not accessible by the Organization.

1. Log Management

RECOMMENDATION

- Identify critical IT systems, determine if system logs are documented and monitored, and establish responsibilities addressing system logging and monitoring procedures.
  - Implement web-based content filtering and facilitate logging of individual employee web traffic
  - Daily monitoring of Core Banking and Network system failed login or unauthorized access attempts
  - Obtain firewall reports and implement processes to review and approve reports to work towards understanding what "normal" on its network looks like.
  - Ensure all remote access sessions are logged, analyzed in a timely manner, and follow-up on any anomalies.
  - Review administrator activity (independent party or IT Committee)
- Ensure audit and security logs be stored on a dedicated Organization server to better facilitate availability in the event an incident requires research.
- Present logs and reports to the IT Committee

1. Log Management

GUIDANCE

- FFIEC Information Security Booklet
  - *II.C.15 Logical Security*
  - *II.C.15(b) Application Access*
  - *II.C.15(c) Remote Access*
  - *II.C.22 Log Management*
- FFIEC Architecture, Infrastructure, & Operations Booklet
  - *VI.B.7 Log Management*
  - *VI.C.3 IT Support*
- NIST SP 800-92: Guide to Computer Security Log Management
- CIS Control 8: Audit Log Management

Log Management Challenges

- Implementation can be complex and time consuming
- Require significant system resources, including storage and processing power
- Maintenance overhead to ensure system remains effective
- Potential for information overload with sheer volume of log data
- Privacy concerns as data can contain sensitive information

Log Management Benefits

- Enhanced Security: Detect and respond to security incidents in real-time
- Improved Compliance: Maintain regulatory requirements by maintaining detailed records of system activities
- Efficient Troubleshooting: Easier to diagnose and resolve issues, root causes
- Operational Insights: System performance and user behavior
- Incident Response and Forensics: Track events leading to incident or breach

2. Multi-Factor Authentication

CONTROL

- Does the Organization require additional security controls around administrative accounts?
  (stronger passwords, additional monitoring, etc.)
- Do additional security controls include multi-factor authentication for all admin access to:
  - Directory services
  - Backup environments
  - Network infrastructure
  - Endpoints/servers

2. Multi-Factor Authentication

OBSERVATION

- The Organization does not require additional authentication controls on administrative accounts or accounts with escalated privileges. These accounts represent the highest risk on the network and should be protected accordingly.
- To mitigate a significant amount of risk, additional authentication controls have been required by FFIEC Guidance Authentication and Access to Financial Organization Services and Systems, and many cybersecurity insurance vendors.

2. Multi-Factor Authentication

RECOMMENDATION

- Identify users, applications and systems who represent a high risk, and for which enhanced authentication controls are warranted to protect information systems.
- Work toward implementing **multi-factor authentication** login requirements (i.e., App-based, mobile push, OTP, token-based) for identified users, applications and systems.
- Elements to consider when identifying high-risk users, applications and systems include:
  - Access to critical systems and data (consider retail e-banking)
  - Cloud-based services (HR platforms, mortgage origination, M365)
  - **Privileged users**, including security administrators
  - Remote access to information systems (employee and vendor access)
  - Key positions such as senior management
- Increase the password length on all administrator accounts to a minimum of **14 characters** with complexity.

2. Multi-Factor Authentication

GUIDANCE

- CIS MS-ISAC Security Primer – Securing Login Credentials
- FFIEC Guidance Authentication and Access to Financial Organization Services and Systems
- Best practice

Risks of Inadequate Authentication Controls

Unauthorized access due to weak authentication measures

Data breaches compromising confidentiality and integrity

Financial loss from hacking and fraud

Reputational damage due to security incidents

Legal consequences of non-compliance with regulations

Operational disruption from unauthorized changes or downtime

3. Microsoft 365 Hardening

CONTROL

- If the Organization has implemented a Microsoft 365 environment, has the Organization had an independent review of the environment since?
- What license does the Organization hold?
- Who manages the environment?

3. Microsoft 365 Hardening

OBSERVATION

The Organization has not contracted for the performance of a Microsoft 365 Hardening Assessment since implementation.

3. Microsoft 365 Hardening

RECOMMENDATION

- Contract for an independent Microsoft 365 Hardening Assessment to evaluate the environment and ensure the Organization has implemented appropriate controls to mitigate risks including:
  - Malware
  - Third-party app access
  - Data loss prevention
  - External sharing
  - Advanced threat protection
  - Permissions

3. Microsoft 365 Hardening

GUIDANCE

- Best practice to perform assessment
- Based upon controls set forth from Center for Internet Security (CIS) Microsoft 365 Benchmarks
  - October 2024 (v4.0)
  - Currently updated every six months

Risks to 365 Configuration Gaps

- **Overprivileged Administrator Roles**:
  - Too many Global Administrators with extensive permissions
  - If compromised, can result in unauthorized access and backdoors
- **Lack of Multi-Factor Authentication**:
  - Exploitation of weak/stolen credentials without additional layer of authentication
- **Phishing Attacks**:
  - Inadequately configured environments become targets
  - Exploit enterprise applications to gain access to data or compromise user accounts
- **Audit Log Neglect**:
  - Lack of monitoring audit logs leave organizations blind to suspicious activity
  - Detection of anomalies and security incidents
- **Authorization Misconfiguration**:
  - Potentially allow external parties unauthorized access to applications
  - Crucial to preventing data exposure

4. Ransomware Self-Assessment Tool

SBS INSTITUTE

CONTROL

Has the Ransomware Self-Assessment Tool (R-SAT) been completed and presented to an authorized committee?

4. Ransomware Self-Assessment Tool

SBS INSTITUTE

OBSERVATION

The Organization has not completed the Ransomware Self-Assessment Tool (R-SAT) released in 2020, and updated to Version 2.0 in October 2023, by the Conference of State Bank Supervisors (CSBS).

The tool is designed for Organizations to assess their efforts to mitigate risks associated with ransomware and to identify opportunities for increasing security.

4. Ransomware Self-Assessment Tool

RECOMMENDATION

- Complete the Ransomware Self-Assessment Tool to assess efforts to mitigate risks associated with ransomware and identify gaps for increasing security
- Review and update accordingly on an annual basis
- Present to the Board or authorized committee (IT)

4. Ransomware Self-Assessment Tool

GUIDANCE

Conference of State Bank Supervisors (CSBS), in conjunction with the Bankers Electronic Crimes Task Force (BECTF) and the U.S. Secret Service

Additional information can be found at:

https://www.csbs.org/ransomware-self-assessment-tool or
https://www.csbs.org/sites/default/files/other-files/NDS-RSAT.pdf

Why the R-SAT?

- False sense of security
- Inadequate mitigation measures
- Raise risk awareness and provides insights
- Identifies gaps
- Provides overview for executive management
- Assists auditors, security consultants, and regulators
- Incorporates lessons learned

5. Artificial Intelligence (AI)

CONTROL

- Is the Organization utilizing Artificial Intelligence (AI) tools as part of regular operations? If so, consider the following:
  - What is the purpose of the Organization's use of AI?
  - Has the Organization considered the licensing associated with the AI tools utilized?
  - Has the Organization documented and approved risk associated with use of the AI tool?
  - Is Artificial Intelligence (AI) addressed within policy (Acceptable Use Policy, Information Security Program, separate policy) and have clear expectations been communicated to employees?

5. Artificial Intelligence (AI)

OBSERVATION

- The Organization has not documented policy, risk, or expectations addressing the use of Artificial Intelligence (AI) within the course of regular business.

5. Artificial Intelligence (AI)

RECOMMENDATION

- Discuss the security risks of Artificial Intelligence (AI) and determine acceptable use within the Organization, including the following:
  - Purpose of AI use internally
  - Identification of tools
  - Licensing
- Identification of possible security risks to protect sensitive data and reputation, risk of data breaches, legal liabilities, regulatory compliance, etc.
- Ensure expectations are documented and clearly communicated to employees

5. Artificial Intelligence (AI)

GUIDANCE

- General Data Protection Regulation (GDPR):
  - While not specific to AI, GDPR impacts AI by regulating data privacy and protection. It requires organizations to ensure that AI systems processing personal data comply with data protection principles
- Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI
  - Signed by President Biden in 2023, this order outlines principles for governing AI in the U.S., focusing on responsible development, security, and ethical use
- White House Blueprint for an AI Bill of Rights
  - This blueprint provides principles aimed at protecting individuals in the context of AI use, including data privacy, algorithmic transparency, and non-discrimination

Top AI Risks & Associated Controls

- Bias in AI Algorithms
  - *Implement an AI governance strategy that includes diverse training datasets, fairness metrics, and regular audits to detect and mitigate bias*
- Cybersecurity Threats (exploitation by malicious actors)
  - *Develop a robust AI security strategy, including risk assessments, threat modeling, and secure-by-design approaches to protect AI systems*
- Lack of Transparency and Explainability
  - *Use explainable AI techniques and tools to ensure transparency and accountability in AI decision-making processes.*
- Data Privacy Concerns
  - *Implement strong data governance policies, including data anonymization, encryption, and strict access controls to protect sensitive information*
- Regulatory and Compliance Risks
  - *Stay informed about evolving regulations and ensure AI systems comply with relevant laws and standards. Establish an AI ethics committee to oversee compliance efforts*

6. Vendor Management

CONTROL

- Does the Organization have a documented Vendor Management Program regarding the acquisition of new IT assets or vendors and the ongoing oversight of third parties and service providers, specifically addressing:
  - Defined risk levels
  - Due diligence required for each risk level and review frequency
  - Contract review processes
  - SOC Reports: Evaluation of Complimentary User Entity Controls
  - Core Providers: Regulatory exam results
  - Fourth-party considerations

6. Vendor Management

OBSERVATION

The Organization has not adequately documented a Vendor Management Program to ensure adherence to 2023 Interagency Guidance on Risks Associated with Third-Party Relationships, the FFIEC IT Booklets, and recommended cybersecurity controls.

6. Vendor Management

RECOMMENDATION

Enhance the Vendor Management Program to comply with 2023 Interagency Guidance on Risks Associated with Third-Party Relationships and FFIEC IT Booklets to encompass the following items:

- Establish clearly defined due diligence procedures addressing the initial review process, documents required, and subsequent annual reviews for vendors dependent on risk categories
- Acquisition procedures should be completed for each new system or asset to be purchased and contain a high amount of due diligence around a number of different vendors or products.
- Define vendor classifications and the corresponding review frequency
- Performance of an annual risk assessment of all vendors to determine criticality
- Report of critical vendor review should be presented to the Board annually
- Establish a contract review process to ensure third-party contracts contain language as recommended by FFIEC Guidance, including scope of service, performance standards, security and confidentiality, controls, audit requirements, reports available for review, business resumption or contingency plans, subcontracting, ownership and license of data, dispute resolution, termination, assignment, regulatory compliance and breach notification procedures.
- Ensure a review of Complimentary User Entity Controls is performed for critical vendors
- Regularly request and review Federal Banking Agency Examination results from the core banking provider
- Consider fourth-party vendors crucial for maintaining a secure and resilient supply chain

6. Vendor Management

SBS INSTITUTE

GUIDANCE

- Interagency Guidance on Risks Associated with Third-Party Relationships (June 2023)
- FFIEC Booklets

Why is Vendor Management so Important?

SBS INSTITUTE

- Cost efficiency
- Enhanced customer experience
- Innovation and agility
- Access to expertise
- Risk mitigation
- Supply chain

7. Backup Processes & Testing

CONTROL

- Does the Organization perform backup and recovery testing annually, including:
  - Restoration testing
  - Functional failover testing?

- Does the Organization maintain **3 backups, on 2 different data types, and one backup offsite**?
- Are the offsite backups **segregated** from the network (air-gapped) and/or **immutable**?

7. Backup Processes & Testing

OBSERVATION

- The Organization does not employ the best practice standard of keeping a copy of all system backups off the network or segmented from the physical network.
- The Organization does not review and test all backups on a regular basis to ensure effectiveness and integrity and validate all information is available and accessible.

7. Backup Processes & Testing

SBS INSTITUTE

RECOMMENDATION

- Rotationally test all critical backups on a regular basis to ensure effectiveness and integrity
- Perform a functional test of the Disaster Recovery and Business Continuity Plan, in particular the Organization should test operational functionality of the backup to ensure operability and efficiency.
- **Keep a copy of all critical systems backups off the network and segmented** (air-gapped) **or immutable** (unable to be altered) to protect from the propagation of ransomware.
- All critical backups should include three copies, on two mediums, with one copy off the network.

7. Backup Processes & Testing

GUIDANCE

- CSBS Ransomware Self-Assessment Tool (RSAT)
- NIST Best Practices – separate locations for backups, testing processes, multiple copies, etc.

Backup Processes and Functional Testing

Risks / Advantages

- Inadequate backups can result in data loss
- Unreliable recovery can occur if backup processes are not thoroughly tested.
- Relying on backups without validating their integrity can lead to false confidence
- Operational delays

- Regular backups ensure data resilience and quick recovery
- Functional testing identifies weaknesses and mitigates risks
- Tested backups support business continuity
- Proper backups align with regulatory requirements
- Functional testing builds confidence in recovery

8. DevOps

CONTROL

Based upon size and complexity of the Organization, has management appropriately developed a SDLC Policy, related procedures, and mitigating controls?

8. DevOps

OBSERVATION

The Organization has not documented a System/Software Development Life Cycle (SDLC) methodology and related procedures to manage systems and system components and achieve objectives of confidentiality, integrity, availability, and resilience to achieve the Organization's business objectives.

8. DevOps

RECOMMENDATION

- Develop frameworks, policies, procedures, and associated controls covering the following:
  - SDLC methodology
  - Project management
  - Acquisition and maintenance
  - Security and controls
  - Data management and data classification
  - Change management
  - Testing and quality assurance
  - Documentation and reporting

8. DevOps

SBS INSTITUTE

GUIDANCE

- FFIEC Development, Acquisition and Maintenance Booklet
- FFIEC Architecture, Infrastructure and Operations Booklet
- NIST SP 800-160 Vol. 1 Rev. 1

Significance of sound practices within DevOps…

- Increased Deployment Frequency
- Faster Recovery from Failures
- Scalability and Flexibility
- Continuous Improvement
- Better User Experience
- Security Integration

- Security Vulnerabilities
- Quality Issues
- Project Delays and Cost Overruns
- Operational Inefficiencies
- Inadequate Documentation
- Poor User Satisfaction

9. Email Security

SBS INSTITUTE

CONTROL

Has the Organization implemented reasonable controls surrounding email security to ensure protection of confidential customer and organizational data?

9. Email Security

OBSERVATION

The Organization has not implemented additional email controls (i.e., DMARC, SPF, encryption) to help ensure the security of sending and receiving email at the Organization.

9. Email Security

RECOMMENDATION

Enhance email security to ensure appropriate risk mitigation related to sending and receiving messages at the Organization:

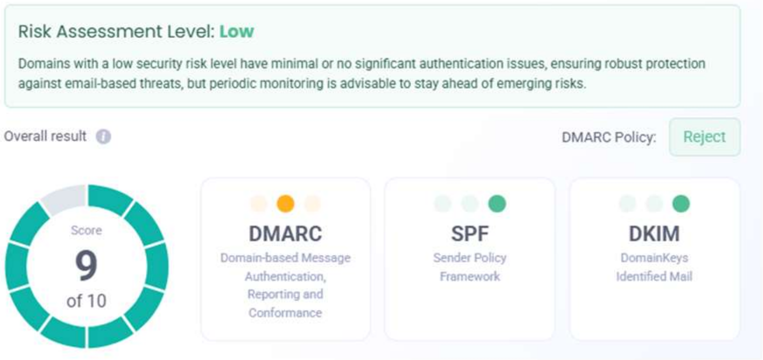
- **Enhanced MFA solution** deployed to authenticate to the application
- **SPF (Sender Policy Framework) -** email authentication method designed to detect forging sender addresses during the delivery of the email. It allows domain owners to specify which mail servers are permitted to send emails on behalf of their domain.
- **DKIM (DomainKeys Identified Mail)** - email authentication method that allows an organization to take responsibility for transmitting a message by signing it in a way that mailbox providers can verify. This verification is made possible through cryptographic authentication.
- **DMARC (Domain-based Message Authentication, Reporting, and Conformance)** - email authentication protocol that helps protect email domain owners from unauthorized use, commonly known as email spoofing. It allows email senders to specify policies for how their email should be handled if it fails authentication checks.
- **Encryption** - Consider platform encryption, secure connections, data at rest, GLBA privacy; discuss with third-party provider; ensure internal conditional access policies

9. Email Security

GUIDANCE

- Center for Internet Security: Microsoft 365 Hardening Standards
- CIS Control 9: Email and Web Browser Protections
- NIST SP 800-177 Rev. 1
- Best practices

- Website to evaluate:
  - www.easydmarc.com



Risk Assessment Level: **Low**

Domains with a low security risk level have minimal or no significant authentication issues, ensuring robust protection against email-based threats, but periodic monitoring is advisable to stay ahead of emerging risks.

Overall result

DMARC Policy: Reject

Score 9 of 10

DMARC Domain-based Message Authentication, Reporting and Conformance

SPF Sender Policy Framework

DKIM DomainKeys Identified Mail

Email Security: Yes, Please

- **Risks**:
  - Implementation Complexity
  - Maintenance and Monitoring
  - Potential for Misconfiguration
  - Performance Overhead

- **Benefits**:
  - Improved Email Deliverability
  - Protection Against Phishing and Spoofing
  - Enhanced Data Privacy and Security
  - Improved Sender Reputation
  - Visibility and Reporting

10. Board Cybersecurity Training

CONTROL

Is cybersecurity addressed in all areas of the Organization, including the **Board of Directors**?

10. Board Cybersecurity Training

OBSERVATION

Cybersecurity training for the Board of Directors has not been completed in the last 12 (twelve) months.

10. Board Cybersecurity Training

RECOMMENDATION

- Train at least annually on Information Security related topics, including:
  - Phishing scams
  - Social engineering threats
  - Physical security
  - Unauthorized access
  - Additional threats pertaining to everyday security of customer information at the Organization
- Document training within Board minutes

10. Board Cybersecurity Training

GUIDANCE

- FFIEC Management Booklet: I.A.2 IT Management
- FFIEC Authentication and Access to Financial Institution Services and Systems (2021)
- FDIC Resources
  - https://www.fdic.gov/banker-resource-center/cybersecurity-resources
  - https://www.fdic.gov/banker-resource-center/pocket-guide-directors

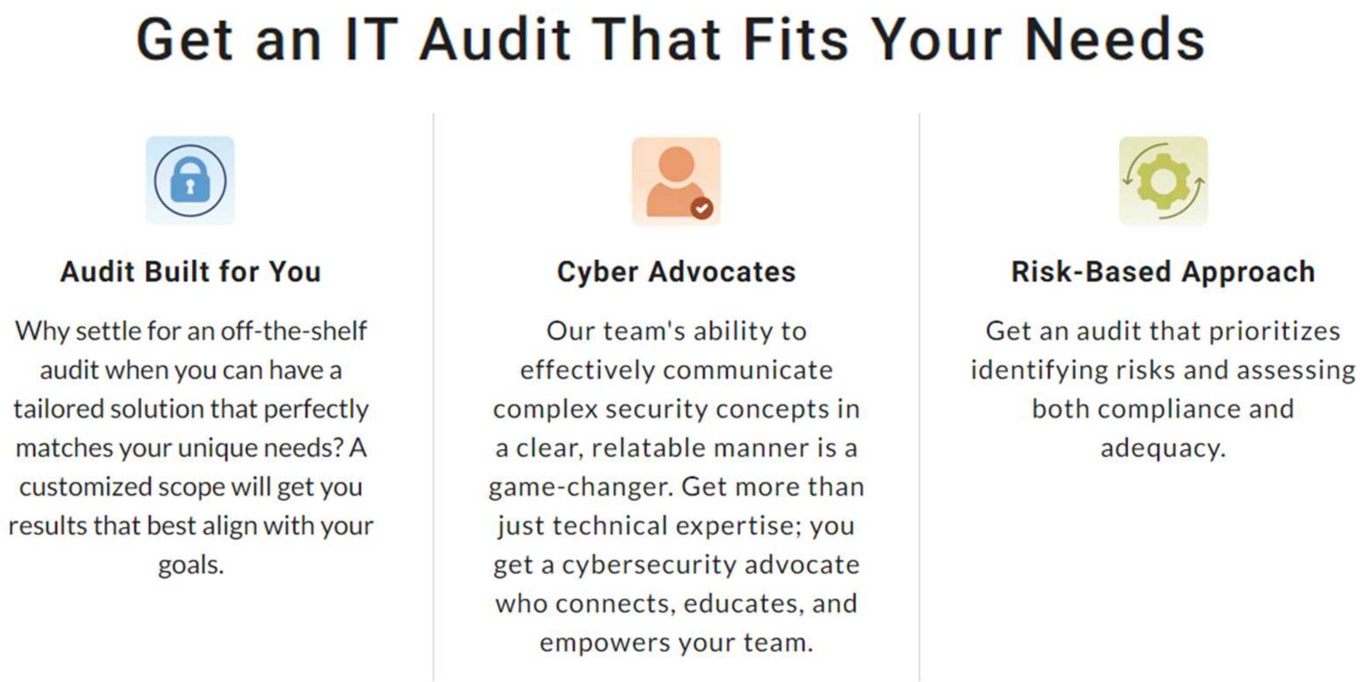
Educate the Board of Directors – Why?

- Inadequate Decision Making
- Failure to Allocate Resources Appropriately
- Misalignment with Business Goals
- Reputational Damage
- Legal and Regulatory Non-Compliance
- Lack of Oversight and Accountability
- Missed Opportunities for Innovation
- Insufficient Crisis Preparedness
- Underestimation of Insider Threats
- Loss of Investor Confidence

Big Audit Recommendation Takeaways

- **Vendor Management**
  - Devil is in the details (CUECs, fourth parties)
  - Comprehensive review of all critical vendors, extra focus on MSPs and cloud
- **Artificial Intelligence…**
  - Determine purposes, define acceptable use, identify risks, develop policy
- **Log Management & Email Security**
  - Ensures effective and efficient monitoring of critical environment aspects, including core, network, firewall, remote access, email, Internet, etc.
- **DevOps**
  - Depending upon complexity and amount of system or software involved, can be fairly straightforward or daunting to wrap arms around; use guidance!
- **Microsoft 365 Environment**
  - With transition to utilizing M365 modules (SharePoint, Teams, OneDrive, etc.) it is critical appropriate security is in place to mitigate any data compromise

Check out SBS's IT Audit Services!



Get an IT Audit That Fits Your Needs

Audit Built for You

Why settle for an off-the-shelf audit when you can have a tailored solution that perfectly matches your unique needs? A customized scope will get you results that best align with your goals.

Cyber Advocates

Our team's ability to effectively communicate complex security concepts in a clear, relatable manner is a game-changer. Get more than just technical expertise; you get a cybersecurity advocate who connects, educates, and empowers your team.

Risk-Based Approach

Get an audit that prioritizes identifying risks and assessing both compliance and adequacy.

https://sbscyber.com/services/it-audit

Learn more about our

Webinar Bundles

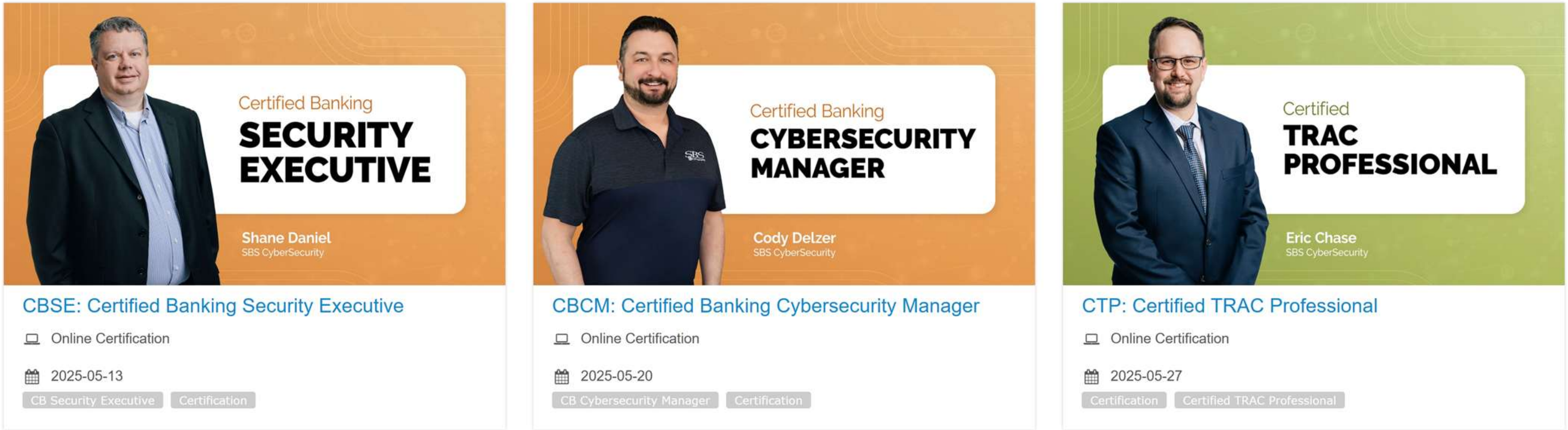
link.sbscyber.com/webinar-bundles

Learn more about

Recertification

link.sbscyber.com/cbsm-recert

SBS Institute Certification Programs



CBSE: Certified Banking Security Executive

Online Certification

2025-05-13

CB Security Executive | Certification

CBCM: Certified Banking Cybersecurity Manager

Online Certification

2025-05-20

CB Cybersecurity Manager | Certification

CTP: Certified TRAC Professional

Online Certification

2025-05-27

Certification | Certified TRAC Professional

link.sbscyber.com/certifications

On-Demand Options Available!

Complimentary Resources

- Posters
- Toolkits
- Infographics
- Tipsheets

10 Key Ideas to Build a

CYBERSECURITY CULTURE

Brought to you by SBS CyberSecurity

Most organizations today realize that they can have the best security money can buy, but if one employee clicks a link or downloads an attachment from an email, all of that security is thrown out the window.

Organizations are providing more and more training and education to their employees to help ensure everyone is doing their part to prevent attackers from gaining access to their networks and stealing information. Follow these tips to build a culture of cybersecurity in your organization

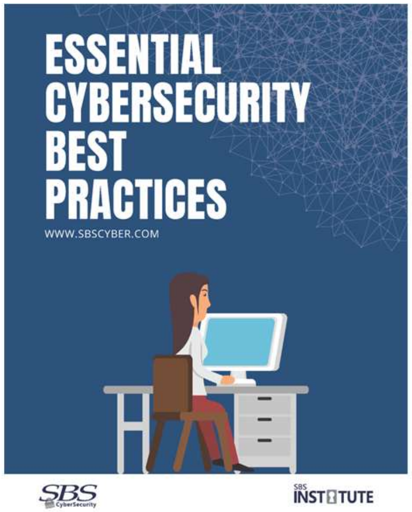
01 START AT THE TOP WITH THE BOARD

A culture of cybersecurity has to start at the top of the organization. The Board of Directors and Senior Management needs to participate in security awareness training and testing. If they don't feel it's important, what message does that send to the rest of the organization?

02 GIVE CYBERSECURITY A STANDING AGENDA ITEM AT EMPLOYEE MEETINGS

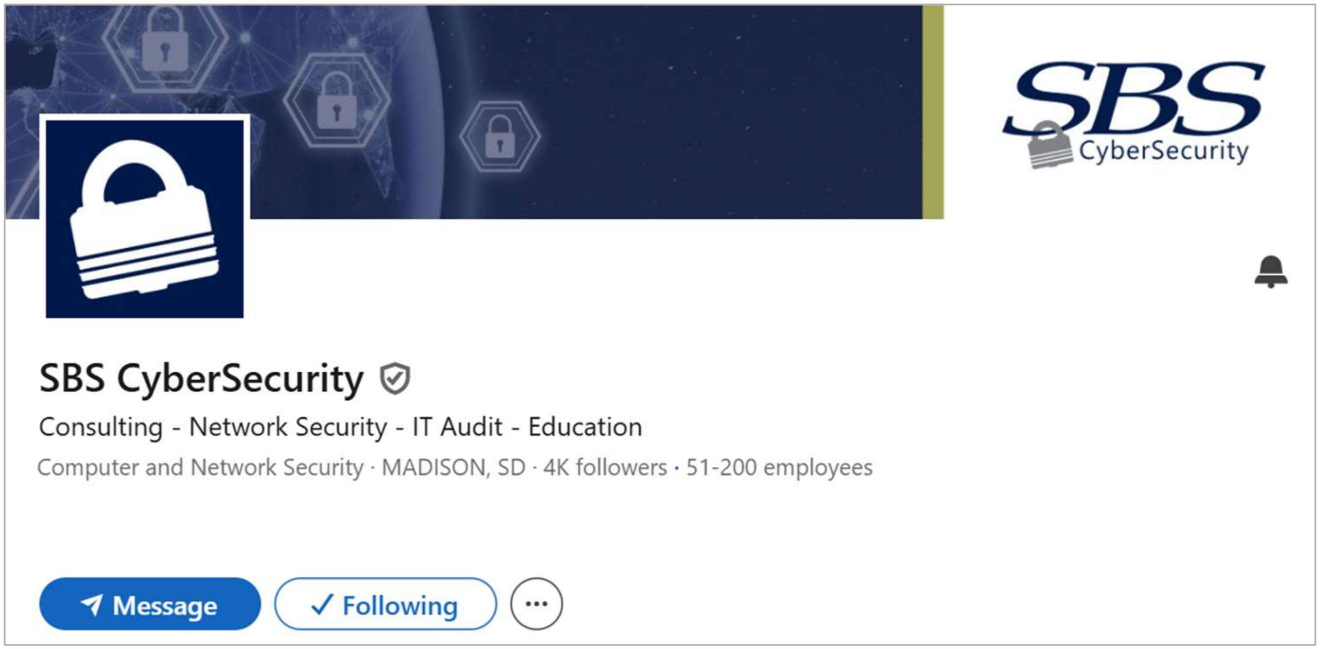
An organization that values cybersecurity talks about cybersecurity at each meeting.

03 TEST YOUR EMPLOYEES REGULARLY



https://learning.sbscyber.com/resourcelibrary

Connect with SBS



SBS CyberSecurity

Consulting - Network Security - IT Audit - Education

Computer and Network Security · MADISON, SD · 4K followers · 51-200 employees

https://linkedin.com/company/sbs-cybersecurity

Cody Delzer

- Principal Consultant
- CISA, CDPSE
- Bachelor's Computer & Network Security from Dakota State University
- Cody.Delzer@sbscyber.com
- 605-228-2829
- www.sbscyber.com

SBS Institute

- sbsinstitute@sbscyber.com
- 605-269-0909