Cybersecurity Essentials for Business Leaders & Aspiring Professionals

CSUF | COLLEGE OF Business and Economics

CYBERFORWARD

Objectives

Welcome to our foundational cybersecurity webinar. Over the next hour, we'll equip you with essential knowledge that will benefit both business leaders and those considering a career in this rapidly growing field.

Understand key cybersecurity threats and how they affect businesses

We'll explore the most common and damaging cyber threats in today's landscape.

Recognize the real-world impact of cyber incidents

Through case studies and examples, see how breaches affect operations, finances, and reputation.

Take away actionable steps to protect your organization

Learn practical measures you can implement immediately to improve security posture.

Explore cybersecurity career opportunities

Discover pathways into the field, regardless of your current background or experience level.

What is Cybersecurity?

At its core, cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These attacks typically aim to:

- Access, change, or destroy sensitive information
- Extort money from users or organizations
- Interrupt normal business processes
- Compromise customer or employee data

Effective cybersecurity requires coordinated efforts throughout an information system, balancing protection with usability to maintain business operations.

Common Threats You Should Know

Understanding these prevalent threats is the first step toward protecting your organization's digital assets.

Phishing

Deceptive emails, messages, or websites designed to steal credentials or install malware. These attacks often mimic legitimate organizations and exploit human psychology.

Example: An email appearing to be from your bank asking you to "verify" account details.

Ransomware

Malicious software that encrypts files or systems, demanding payment for the decryption key. Ransomware can bring operations to a complete halt.

Example: Colonial Pipeline paid $4.4 million after a 2021 attack disrupted fuel supplies.

Insider Threats

Current or former employees, contractors, or business partners who misuse their authorized access to critical assets, either maliciously or accidentally.

Example: An employee downloading sensitive customer data before leaving for a competitor.

Social Engineering

Psychological manipulation to trick users into making security mistakes or giving away sensitive information, often bypassing technical security measures.

Example: Impersonating IT support to gain remote access to a computer.

The CIA Triad + Privacy: Core Security Principles

Confidentiality

Ensures sensitive information is accessible only to authorized individuals. Implemented through encryption, access controls, and authentication measures.

Integrity

Maintains the accuracy and trustworthiness of data throughout its lifecycle. Protected via checksums, version control, and digital signatures.

Availability

Guarantees reliable access to information and systems when needed. Ensured through redundancy, backups, and disaster recovery planning.

Privacy

Ensures individuals and organizations control how their personal data is collected, used, and protected. It's about respecting user rights and meeting regulatory obligations (GDPR, CCPA, etc.).

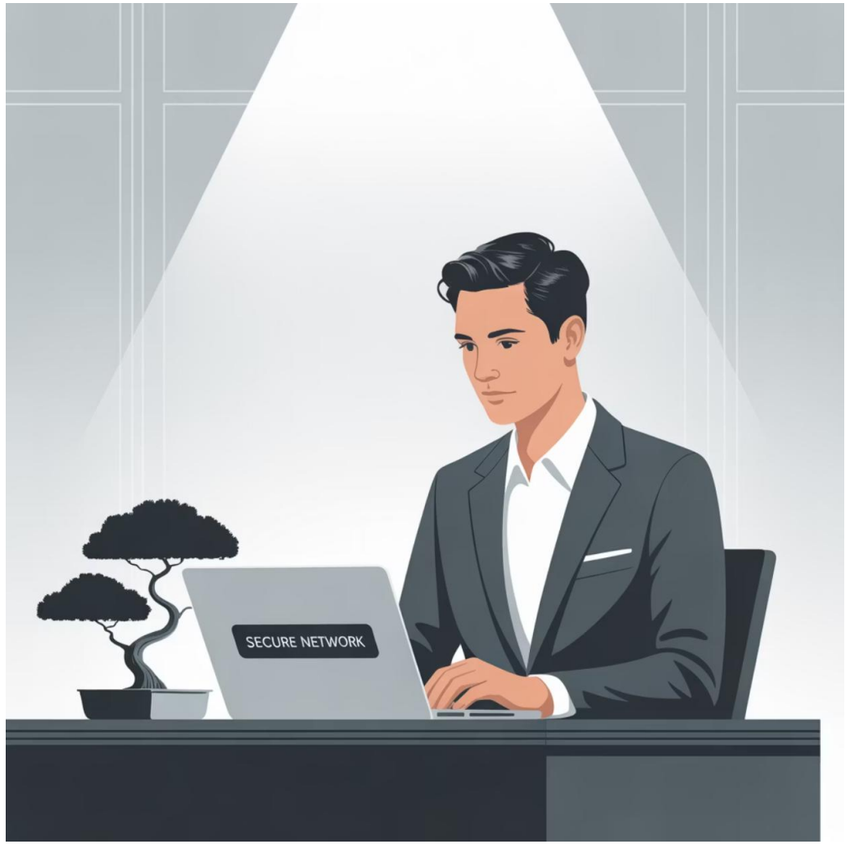
These three principles form the foundation of every effective cybersecurity program. A weakness in any one area compromises the entire security posture.

Let's examine where cybersecurity matters most in your daily operations

Cybersecurity in Daily Business Operations

Modern business operations rely heavily on digital systems, creating numerous security touchpoints that require protection:

- **Cloud services** - Where is your data stored? Who has access? → Access controls
- **Email communication** - The primary vector for phishing attacks → Security training
- **Mobile devices** - Both company-issued and personal (BYOD) → Device management
- **Remote work** - Home networks, public WiFi vulnerabilities → VPN protection
- **Third-party integrations** - Vendors with access to your systems → Vendor assessment



Did you know? Human error is involved in more than 85% of data breaches, making employee training one of the most cost-effective security measures.

Quick Wins for Cyber Hygiene

These high-impact, low-effort security measures can dramatically improve your protection against common threats:

Enable Multi-Factor Authentication (MFA)

Requires something you know (password) and something you have (like a phone) to access accounts. MFA blocks 99.9% of automated attacks, according to Microsoft.

Action: Enable MFA on email, financial, cloud storage, and social media accounts immediately.

Use a Password Manager

Creates and stores unique, complex passwords for each service. Prevents credential reuse across sites and makes phishing more difficult.

Action: Set up a reputable password manager like 1Password, LastPass, or Bitwarden for your team.

Regular Updates

Software updates patch security vulnerabilities. Unpatched systems are like unlocked doors for attackers.

Action: Implement automatic updates where possible and establish a regular update schedule.

Security Awareness Training

Regular training reduces human error and builds a security-conscious culture. Simulated phishing tests can reduce click rates by 50%.

Action: Schedule quarterly training sessions and monthly security reminders for all staff.

Audience Activity: Threat Modeling Exercise - TechServe Inc.

Time to think like a security professional!

This exercise helps us identify weaknesses before real attackers do.

Step 1: Identify Defense Gaps

As a business leader, where are your current security gaps? Consider areas like access controls, data protection, employee training, or patching schedules?

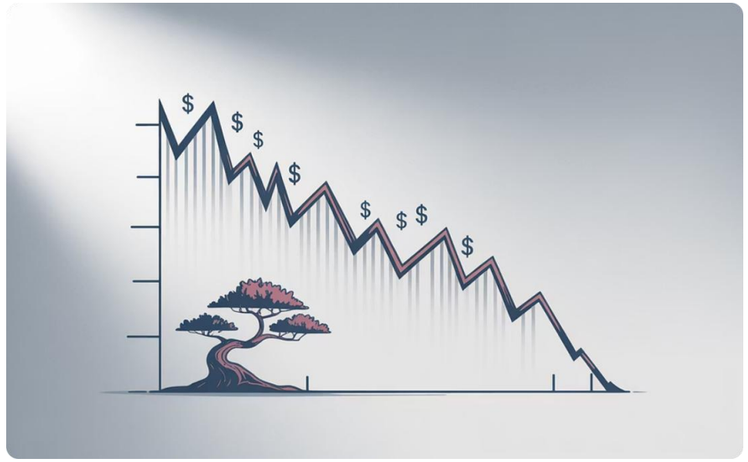
Step 2: Attacker's Perspective

Now, imagine you're a security professional conducting a penetration test. How would you exploit the defense gaps you just identified? Consider how weak passwords, outdated systems, or insecure remote connections could be leveraged.

This exercise demonstrates the value of threat modeling - systematically identifying potential threats to better prioritize your defenses.

Impact of Cyber Incidents on Business

Cybersecurity is not just an IT issue - it's a business risk with far-reaching consequences.



Financial Losses

The average cost of a data breach in 2025 reached $4.44 million. This includes investigation costs, ransom payments, system recovery, and business downtime.

Reputational Damage

Customer trust takes years to build but moments to destroy. 65% of customers report losing trust in companies after a breach affecting their personal data.

Regulatory Penalties

GDPR fines can reach €20M or 4% of global revenue. In the US, sector-specific regulations like HIPAA can impose penalties up to $1.5M per violation category.

Case Study: The 2013 Target breach affected 41 million customers and cost over $200 million in settlements, upgrades, and legal fees. Their stock dropped 46% and their CEO resigned.

Leadership's Role in Cybersecurity

Effective cybersecurity requires top-down commitment

Leaders set the tone for the entire organization's security culture. When executives prioritize security, employees follow suit.

Strategic Resource Allocation

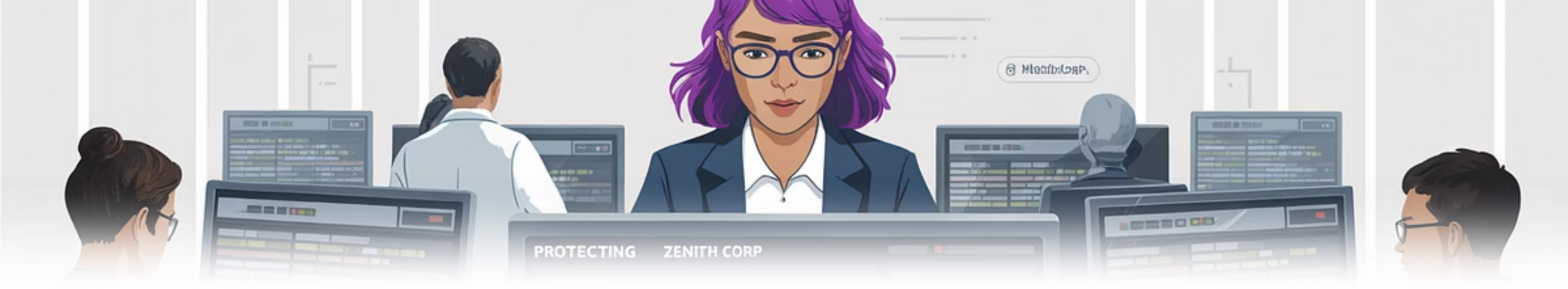
Invest appropriately in security tools, training, and personnel based on risk assessment, not just after incidents occur.

Business-Aligned Security

Ensure security measures support rather than hinder business objectives; balance protection with operational needs.

Crisis Leadership

Develop and regularly test incident response plans; be prepared to make critical decisions under pressure when breaches occur.



Cybersecurity Careers: An Overview

4.8M

Global Job Shortage

Unfilled cybersecurity positions worldwide in 2024 ISC2

$135K

Average Salary

For US cybersecurity professionals

The cybersecurity field offers exceptional career prospects across all experience levels and backgrounds. Contrary to popular belief, many roles don't require deep technical expertise - critical thinking, communication, and business acumen are equally valuable skills for many positions.

Popular Cybersecurity Roles

Security Analyst

Responsibilities: Monitor security systems, investigate alerts, respond to incidents, document security events

Skills: Threat detection, incident response, log analysis, security tools

Salary Range: $70,000 - $115,000

Entry-level friendly: Yes, with right certifications

Penetration Tester

Responsibilities: Simulate attacks to find vulnerabilities, document findings, recommend fixes

Skills: Ethical hacking, security tools, scripting, clear reporting

Salary Range: $90,000 - $160,000

Entry-level friendly: Usually requires experience

GRC Analyst

Responsibilities: Ensure compliance with regulations, develop policies, conduct risk assessments

Skills: Regulatory knowledge, documentation, process improvement

Salary Range: $75,000 - $120,000

Entry-level friendly: Yes, especially for those with business background

CISO

Responsibilities: Develop security strategy, oversee security operations, report to board, manage security budget

Skills: Leadership, business acumen, risk management, communication

Salary Range: $175,000 - $300,000+

Entry-level friendly: No, senior executive position

Certifications to Get You Started

Industry certifications validate your knowledge and demonstrate commitment to potential employers.

CompTIA Security+

The gold standard entry-level security certification. Covers fundamental security concepts and best practices.

Difficulty: Moderate | **Cost:** ~$370 | **Study time:** 1-3 months

ISC2 SSCP

Focused on security operations and monitoring. Great for those interested in hands-on security roles.

Difficulty: Moderate | **Cost:** ~$249 | **Study time:** 2-4 months

ISC2 Certified in Cybersecurity (CC)

Entry-level certification covering security principles, incident response, and governance.

Difficulty: Beginner | **Cost:** ~$249 | **Study time:** 1-2 months

Learning Resources

- **TryHackMe** - Interactive cybersecurity training with guided paths
- **IBM SkillsBuild** - Free courses and badges in security fundamentals
- **Cybrary** - Extensive library of free cybersecurity courses
- **SANS Cyber Aces** - Free online courses in cybersecurity essentials
- **CISA Cybersecurity Training** - Government-provided free resources
- **CyberForward –** Foundational knowledge and skills development

Getting into the Field: Next Steps

Build Your Knowledge Foundation

- Assess where you are in your learning journey (TPS, Skill IQ)
- Complete free online courses (TryHackMe, Cybrary)
- Read security blogs, newsletters, and reports

Join the Community

- Participate in LinkedIn groups and X/Thread/BlueSky discussions
- Join Discord servers like "Cybersecurity" and "The Many Hats Club"
- Attend local meetups and virtual conferences

Gain Practical Experience

- Participate in Capture The Flag (CTF) competitions
- Contribute to open-source security projects
- Apply for internships, even in adjacent IT roles

Land Your First Role

- Leverage related experience (IT, compliance, etc.)
- Apply for SOC Analyst, Jr. Security Analyst positions
- Consider security-adjacent roles as entry points

Remember: Cybersecurity is a rapidly evolving field. Continuous learning and adaptability are essential for long-term career success.

Final Thoughts & Q&A

Key Takeaways

Cybersecurity is a business imperative

Not just an IT issue, but critical to business continuity, reputation, and bottom line.

Simple actions make a big difference

MFA, password management, updates, and training address most common threats.

Career opportunities are abundant

The field needs diverse talent and offers multiple entry paths regardless of background.

CYBERFORWARD

Thank You!

Stay aware, stay secure!

Contact us:

Dr. Rahul Bhaskar: rbhaskar@fullerton.edu

Dr. Sinjini Mitra: smitra@fullerton.edu

Website: https://business.fullerton.edu/

CSUF | COLLEGE OF Business and Economics

Maurice Gibson: Maurice.Gibson@cyberfwd.com

Website: https://cyberfwd.com/

CYBERFORWARD