



Anti-CyberCrime Team Training Services, LLC
8511 Knox Avenue South
Bloomington, MN 55431-1774
(952) 888-1108

bob@ACCTTS.com

ACCTTS: **Anti-CyberCrime Team Training Services**

Providing Information Protection Education -Training Programs & Support Services

ACCTTS Services

ACCTTS provides the **Information Protection Team Training Series (IPTTS)**, a comprehensive series of courses designed to educate senior executives, IT staff, and employees in security best demonstrated practices. This education series addresses management concerns about reliable information assurance and intellectual property protection.

It also provides adult learners with the skills and knowledge needed to prevent and combat CyberCrime.

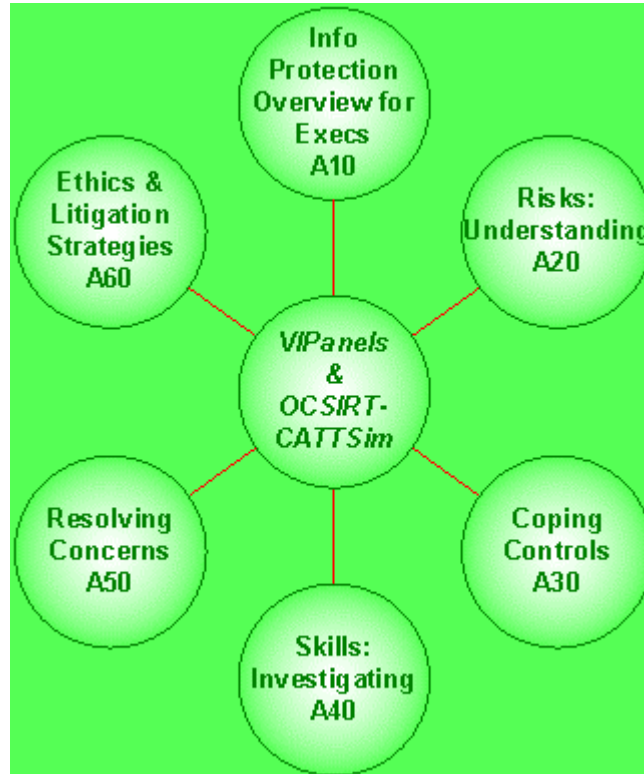
The series answers these questions:

- *What is required to protect information assets?*
- *Why is security personally & professionally relevant?*
- *How do you effectively integrate **People, Policy and Process** into an effective security policy?*
- *How do you avoid losing the **TRUST** of your stakeholders and trading partners?*
- *Where mandated, how do you comply with regulations & laws to avoid legal sanctions or fines?*



Syllabus

Each of our courses integrates information protection expertise with education and team training programs. These programs include lively presentations and interactive workshops.



1. Information Protection Overview

The Information Protection Overview Series introduces basic CyberCrime and CyberEthics concepts to executives and other non-technical employees.

This series serves as an introduction to CyberCrime concepts for all employees and stakeholders and forms a basis for further training in other ACCTTS courses such as **Understanding Risk Factors**. The following are course titles in this series. See course details in the following sections.

A11A: *Quick Intro to CyberCrime Fighting for All Stakeholders*

A11S: *Information Protection Overview (for Executives)*

A12A: *Introduction to CyberEthics for All Stakeholders*

A12S: *Introduction to CyberEthics for Senior Management*



2. Understanding Risk Factors

The Understanding Risk Factors Series delves more deeply into Who, What, and Why CyberCrime Happens. The following are course titles in this series. See course details in the following sections.

A21A: *Introduction to Understanding Information Security for All Stakeholders*

A21S: *Introduction to Understanding Information Security for Sr. Management*

A22: *Building an Information Security Awareness Program (ISAP)*

A23: *Security Technologies Program (STP)*

3. Coping Controls

The Coping Controls course provides participants the skills and knowledge to manage or support the critical aspects of enterprise Information Assurance and Network Security.

4. Investigating Skills

Investigating Skills participants learn how to acquire, protect and analyze digital evidence from Cyber Crimes. Reinforces effective Security Incident Response Team (SIRT) tactics.

5. Resolving Concerns

Resolving Concerns participants learn how to analyze situations and implement solutions. The focus is on managing business disruptions, determining their root causes and effects. It also helps reinforce and strengthen any organization's information protection programs.

6. Litigation Strategies

Litigation Strategies participants learn how to design, develop and effectively prosecute (civil or criminal) Cyber Crimes involving digital disruptions to business as usual.



Course Details

1. Information Protection Overview (for Executives)

Overview

The Information Protection Overview course focuses on key business and legal issues driving global requirements for more effective Information Protection and Network Security.

Information Protection Overview establishes the foundation for the complete **Information Protection Team Training Series** with its focus on **People, Policy and Process**. It forms the foundation for further ACCTTS courses such as [Understanding Risk Factors](#).

Who Should Attend

- Executives, Directors & Senior Managers responsible for crafting or maintaining Enterprise Information Protection Strategies & Policies.
- Any persons who must implement or monitor Information Assurance and Privacy Policy Decisions.

Job Title examples include the following or direct reports of:

- **Chief Executive Officer**
- **President**
- **Chief Compliance Director**
- **Chief Operating Officer**
- **Chief Knowledge Officer**
- **Chief Privacy Officer**
- **Chief Legal Officer**
- **Chief Financial Officer**
- **Chief Information Officer**
- **Executive Vice Presidents**
- **Vice Presidents**
- **Outside Counsel & Advisors**

Courses in This Series

A11A: *Quick Intro to CyberCrime Fighting for All Stakeholders*

Simple Computing Safeguards for Small Business and Home Computer Users

Concepts covered:

- Password protection practices



- Using strong (non-shared) authentication
- Making regular backups of critical data
- Using effective software protection from malware

malware

(MALicious WARE) Software designed to destroy, aggravate and otherwise make life unhappy or frustrating. See virus, macro virus, Word macro virus, Worms and Trojan horse

- Proper email procedures
- Secure home office connectivity policies
- Understanding firewalls and gateways
- Resources to help educate and protect

A11S: *Information Protection Overview (for Executives)*

Overview

This orientation session is designed for non-technical executives and professionals who need to understand the key business issues and compliance laws driving their organization's information protection and network security practices. At the end of the four-hour seminar, you will know how to evaluate the effectiveness of your organization's information security policies. Learn the right questions to ask your staff. Understand the risks that cyber crimes and cyber terrorist attacks pose for your organization. Find out what can be done to prevent attacks and to minimize their impact. Sample corporate information security policies are also included that you can take back to use in your organization.

The course uses real world examples to show how competitors or Cyber-criminals may compromise data integrity or disrupt your network's availability and reliability. It anchors our team training series with a focus on **People, Policy and Process**.

Focus

- Participant workshops reinforce both risk assessment and mitigation methods in a straight-forward common sense format with a take-home executive risk assessment checklist and policy template.
- Overview and guidelines for preparing, responding to and following-up after digital disruptions.



Who Should Attend

The audience for this course includes:

- **CEOs**
- **CIOs**
- **Presidents**
- **Directors**
- **Compliance Officers**
- **Senior Managers**
- **Anyone responsible for crafting enterprise information protection strategies & policies**

Outcomes

What you will learn:

- Are we at risk?
- Who and what are the threats?
- How do we prepare for the inevitable?
- How do we determine if we have been attacked?
- How do we stop an attack in progress?
- What do we do?
- Who do we notify?
- How do we recover from an attack?

Outline

Section	Topic
1	Course Objectives & Overview / CBS "Cyber Thief" Video (15 Min)
2	Cyber Crime: A Most Unnatural Disaster
3	An Ounce of Prevention - <i>AVOID Being Victimized!</i>
4	Breakout-1: Assessing Risks & Security Incident Response Team (SIRT) Preparation
5	Prudent Protection Practices & Safeguards
6	A Pound of Cure - Detection and Correction
7	Breakout-2: Responding to "Cyber Attack" - Digital Disruption Simulations
8	Forensics & Dr. Quincy, ME - Analyzing Root Causes
9	Q&A Review with Overall Evaluation



Length

1/2 Day

Materials

Workbook, Workshop Guide & Information Protection Policy Templates

A12A: *Introduction to CyberEthics for All Stakeholders*

Overview

This half-day seminar introduces participants to CyberEthics, the ethical possibilities and dangers in the developing IT world. This practical course gives day-to-day network users basic knowledge and tools to engage evolving ethical issues of appropriate network use, and appropriate response to misuse. Participants will emerge motivated and equipped to be careful and proactive.

Focus

The course shows how the smallest network action or event can have wider consequences. Consequences can be positive or negative, and affect not just for the person(s) involved, but for the whole organization. Participants learn to identify these ethical situations, and leverage their new knowledge for positive outcomes.

Who Should Attend

This course is designed for any routine users of Web/Internet-based communications and business systems. It is particularly appropriate for sales personnel, account managers and administrators, and PR staff.

Outcomes

Participants will:

1. Gain a basic knowledge of ethical theory and processes.
2. Better understand the implications and impact of cyber-based work.
3. Gain first stage knowledge of ethics in a cyber environment.
4. Feel equipped to recognize and evaluate emergent issues.
5. Understand the need to be proactive and careful within the vision and structure of their corporation.



6. Learn practical rules and principles to apply in the cyber world (based on the Brookings Institute's Ten Commandments for CyberEthics).

Method and Materials

The seminar employs a mix of exercises, case studies, and small group work to provide, memorable, hands on, team based learning.

In order to encourage review and continuing education, course materials include:

1. A complete summary of the classwork
2. Three self-administered exercises
3. A short and straightforward bibliography and reference list.

A12S: *Introduction to CyberEthics for Senior Management*

Overview

This two-hour seminar gives corporate leaders an overall understanding of the evolving impact of CyberEthics, and the means to lead and make sense of an increasingly fragmented medium.

Focus

The focus of this seminar is threefold

1. Understanding the dangers and possibilities inherent in global, unregulated Cyber business
2. Leading and managing with vision in an area where rules address only yesterday's issues.
3. Providing information and strategies for coherent, ethical and proactive corporate response to emergent cyber issues.

Who Should Attend

- The course is most suited to those generating corporate vision and policy, and the senior managers who implement it.

Method and Materials

- Presentations and discussion are reinforced by three exercises providing common experience for participants to reflect upon, individually and in small teams, during the seminar and later.



- Comprehensive written resources accompany the seminar.

Topics

- Ethics - a survey of principles and practice before the IT revolution.
- CyberEthics - principles and practice after the IT revolution.
- Compliance and reaction versus proactivity - the case for visionary policy in a rapidly changing environment.

The way forward: possible strategies and principles, defensive and preemptive, to move more confidently into the CyberEthical world.



2. Understanding Risk Factors

Understanding Risk Factors delves more deeply into Who, What, and Why CyberCrime Happens.

Programs in this series answer these questions:

- What is really required?
- Why is it personally relevant?
- How to implement & improve your defense in depth practices?

Understanding Risk Factors serves as a base of knowledge for all employees and stakeholders in preventing CyberCrime and in protecting intellectual property. It forms the basis for further ACCTTS courses such as [Coping Controls](#)

Who Should Attend

- Department Managers
- Project Managers
- Contractors
- Suppliers
- Current or potential members of a Security Incident Response Team (SIRT)
- All employees directly or indirectly involved with information vital to business success

Job Title examples include the following or direct reports of:

- **Chief Executive Officer**
- **President**
- **Chief Compliance Director**
- **Chief Operating Officer**
- **Chief Knowledge Officer**
- **Chief Privacy Officer**
- **Chief Legal Officer**
- **Chief Financial Officer**
- **Chief Information Officer**
- **Executive Vice Presidents**
- **Vice Presidents**
- **Outside Counsel and Advisors**

And Staff of:

- Accounting
- Human Resources
- Customer Services
- Risk Management
- Warehouse
- Marketing and Sales



A21A: *Introduction to Understanding Information Security for All Stakeholders*

Overview

This program provides an overview of what Information Security covers, today's threats, and what you need to be aware of.

This introduction presents a few case studies of factual incidents, how organizations were affected, and what they did to improve their Information Security Posture.

It includes a brief overview of how the CyberCriminal works and some of their typical behavior patterns plus a consideration of today's internal threats.

Who Should Attend

- All employees

Outcomes

Participants will have a high level understanding of:

- What is Information Security?
- What threats exist
- Some popular CyberAttack methods
- Who and where are the threats?
- What you can do to improve your Information Security Posture
- Recommended sites, tools, references & resources

Length

2 Hours

Materials

Workbook & Case Studies



A21S: *Introduction to Understanding Information Security for Sr. Management*

This program provides an overview of what Information Security covers, typical threats and what Senior Management team members need to be concerned about.

This briefing presents case studies of factual incidents, how organizations were affected, and what management did to improve their Information Security Posture.

This course explains why management must perform due diligence in this area. It also includes a brief overview of how the Cyber Criminal works, some related behavior patterns plus an understanding of today's internal threats.

Who Should Attend

- Executive and Corporate Management
- CEO
- President
- CIO
- Chief Marketing Officer
- Vice Presidents

Outcomes

Participants will have a high level overview & understanding of:

- What Information Security is and the threats to the organization
- Common CyberAttack methods used
- What to do to ensure due diligence is understood in the enterprise
- Recommended sites, tools, references and resources for your IT Staff to assess

Length

2 Hours

Materials

- Workbook
- Case Studies
- Reference Guide



A22: *Building an Information Security Awareness Program (ISAP)*

Overview

This program provides information on how to build an Information Security Awareness Program (ISAP) from the ground up. It includes various methods and ways to present essential information plus links to resources that can help you.

This information enables you to create an Information Security Awareness Program with a limited budget (except your time) up to a more comprehensive program without funding limits.

Who Should Attend

- Human Resources Staff
- Employees Responsible for Awareness Programs
- Security Analysts
- IT Security Staff
- IT Security Manager

Outcomes

Participants will demonstrate a high level understanding of:

- What is Information Security is and the threats to the company
- Typical CyberAttackmethod demonstrations or illustrations
- What to do to ensure prudent protection practices are used in the organization
- Recommended sites/tools/references for your IT Staff to evaluate

Length

1 Day

Materials

- Workbook
- Case Studies
- Security Awareness Program Templates



A23: Security Technologies Program (STP)

Overview

This technology support team training program provides an overview of proven practices that help to protect your digital information assets and interconnecting network(s).

It includes practical case studies plus a reference listing of current references for specific safeguard suppliers and their products.

Who Should Attend

- Security Analysts
- Network Administrators
- Network Managers

Outcomes

Participants will receive a solid understanding of baseline IT Security Safeguards such as:

- Tokens
- Firewalls
- Routers
- DMZ's
- Server security
- Biometrics
- SSL
- Encryption

Length

2 Days

Materials

- Workbook
- Case Studies
- Reference Guide



3. Coping Controls

Overview

The Coping Controls course focuses on methods to prevent and protect against cyber crime and cyber terrorism, to detect and respond to intrusions, and to handle a variety of attacks, viruses, and worms. It provides the skills and knowledge related to the most critical aspects of Information Assurance and Network Security. Program participants will know how to implement realistic safeguards that ensure timely, organized, and effective responses to disruptive cyber crime and cyber terrorist attacks.

Who Should Attend

- Key persons who are current or potential members of a Security Incident Response Team (SIRT).
- Employees with some experience in:
 - Operational auditing
 - Business continuity/disaster recovery
 - Customer service
 - Fraud investigation
 - Litigation support
 - Network technical support
 - Information security or risk management
- IT technical staff or support roles

Job Title examples include the following, direct reports or Staff of:

- **Chief Information Officer**
- **IT Audit Services Director**
- **Information Security Director**
- **Corporate Security Director**
- **Legal Department Director**
- **Law Enforcement Liaison**
- **Computer Platform Specialists**
- **Network Managers**
- **Network Administrators**
- **Financial Auditor**
- **Fraud Examiner**
- **Public Relations Staff**
- **Human Resources Staff**

Outcomes

Program participants learn how to implement realistic safeguards that ensure timely, organized, and effective responses to digital disruptions affecting operational service levels.



4. Investigating Skills

Description

This seminar focuses on how to conduct full-scale investigations of CyberCrime and CyberTerrorism incidents. Participants learn how to acquire and analyze evidence from incidents plus how to implement best practices that are essential to the availability, integrity and confidentiality of critical information assets.

Who Should Attend

Job Title examples include the following, direct reports or Staff of:

- **Chief Information Officer**
- **IT Audit Services Director**
- **Information Security Director**
- **Corporate Security Director**
- **Legal Department Director**
- **Law Enforcement Liaison**

And:

- Computer Platform Specialists
- Network Managers Network Administrators
- Financial Auditor
- Fraud Examiner
- Public Relations Staff
- Human Resources Staff

Outcomes

Investigating Skills participants learn how to acquire, protect and analyze digital evidence from Cyber Crimes. Reinforces effective Security Incident Response Team (SIRT) tactics.

Participants also learn how to quickly assess and improve prudent business practices essential to safeguarding the availability, integrity and confidentiality of mission critical information assets.



Resolving Concerns

Description

Resolving Concerns addresses incident causes, effects, and solutions in order to reinforce and strengthen information protection programs. Learn how to select and apply effective process and technology improvements based on SIRT (Security Incident Response Team) investigative results.

The focus is on managing business disruptions, determining their root causes and effects.

The course also helps reinforce and strengthen any organization's information protection programs.

Intended Audience

Job Title examples include the following or direct reports of:

- **Chief Information Officer**
- **IT Audit Services Director**
- **Information Security Director**
- **Corporate Security Director**
- **Legal Department Director**
- **Law Enforcement Liaison**

And the Staff of:

- Chief Executive Office
- President
- Chief Compliance Director
- Chief Operating Officer
- Chief Knowledge Officer
- Chief Privacy Officer
- Chief Legal Officer
- Chief Financial Officer
- Chief Information Officer
- Executive Vice Presidents
- Vice Presidents
- Outside Counsel & Advisors

Outcomes

Resolving Concerns participants learn how to analyze situations and implement solutions.



Participants understand how to select and integrate effective process or technology improvements based on insights from Security Incident Response Team (SIRT) investigative reports.



Litigation Strategies

Description

Litigation Strategies participants learn how to design, develop and effectively prosecute (civil or criminal) CyberCrimes involving digital disruptions to business as usual.

Participants understand how to recycle results of Security Incident Response Team (SIRT) deliverables as feedback for improving prudent information protection policies and practices.

Intended Audience

Job Title examples include the following or direct reports of:

- **Chief Compliance Officer**
- **Chief Legal Officer & Staff**
- **Outside Legal Counsel**
- **Computer Platform Specialists**
- **Network Managers**
- **Financial Auditors**
- **Fraud Examiner**

And the Staff of:

- Human Resources Staff
- Public Relations Staff



Anti-CyberCrime Team Training Services, LLC
8511 Knox Avenue South
Bloomington, MN 55431-1774
(952) 888-1108

bob@ACCTTS.com