Jonathan Taormina, CPP, CFE, PCI

POA – SECURITY MANAGEMENT

CHAPTER 1 ADMINISTRATIVE MANAGEMENT PRINCIPLES

- Security Managers – security specialists and business managers.
    - Understand business principles – business partners.
    - Support business goals – develop metrics.
    - Management-defined business processes to support the business.
- Organizational Strategy (Strategic Plan)
    - In writing, by BU's top leadership.
    - General direction and long-term goals.
    - 3-5 year view.
    - SWOT – Strengths, Weaknesses, Opportunities, and Threats.

Communicating the Strategy

- Vision – specific description of where the business will be in the long-term.
- Mission – specifies types of products/services, quality, and tangible aspects.
- Objectives – specific goals or other relevant metrics, that must be SMART.
    - SMART – Specific, Measureable, Attainable, Relevant, Time-Bound.

Principles of Business Administration

- primary resource = People.
- Business principles define how an organization functions:
    - Human resource requirements, knowledge management, and corporate structure.
- Human Resource Management:
    - Talent acquisition.
    - Training and performance measurement.
    - Staffing is most visible function.
        - Effective job requirements analysis.
        - Direct and Indirect requirements. Indirect requirements increase the likelihood of the candidate's success.
            - Leadership ability, multitasking, organizational skills, communication skills.
    - Leadership, management and interpersonal skills.
    - Internal recommendations are best way to recruit.
- Policies and Procedures:
    - Policies – items the organization monitors. All must comply. (Compliance can be accomplished through training/certification).
    - Procedures – deal with specific items. (Important to daily function).
- Performance Measuring and Testing:
    - Training mechanisms for employee growth.
    - Performance metrics and training modules.
    - Metrics should align with organizational strategy.
    - How well they do their job AND contribute to company growth.

- Knowledge Management
  - Corporate knowledge is 2nd most valuable resource.
  - Central Knowledge Management System:
    - Collects, distributes, and publicizes corporate data.
  - Used to collect data to measure productivity of the business units and individual employees.
  - Cross-Unit Knowledge Sharing – learn from ideas of another unit.
- Corporate Structure
  - Structured to support business strategy.
  - Aids in delegating responsibility and ensuring accountability.
  - Must identify the essential business units.

Management practices must be aligned with the strategic plan.

- expressed through:
  - Human resource management.
  - Knowledge management.
  - Business structure.
- Overall corporate strategy must be ingrained in daily administration practices.

Jonathan Taormina, CPP, CFE, PCI

CHAPTER 2 FINANCIAL MANAGEMENT

- Understanding the accounting principles used in generating financial reports.
- Financial analysis is used to develop budgets and set expected goals for revenue or return on investment (ROI).
- Public traded AND privately owned companies must follow accounting and financial reporting standards.

Financial Strategy

- management's financial approach to determining the expected returns of its investments and estimating and managing the relevant risks.
- Identify expected margins – the profit that businesses make.
  - Reduce costs or increase prices.
- How to fund growth? – internal cash reserves or commercial financing and investors.

Financial Statements

- created in accordance with Generally Accepted Accounting Principles (GAAP).
  - Establishes a standard for financial reporting.

Income Statement

- How much money an organization generates (revenue),
- How much it spends (expenses),
- Difference between those figures (net income).

- Expenses = cost of goods sold, sales and marketing, administrative, interest, and taxes.
- EBITA – earnings before interest, taxes, and amortization.
- Aids in assessment of overall financial health.

Balance Sheet

Assets = Liabilities + Shareholder Equity

- Asset – anything a company owns or has title to that may provide a futeure economic benefit.
- Liabilities – financial commitments (loans, bills, obligations).
- Shareholder Equity – amount of ownership allocated to shareholders.
  - Not an asset or liability.
  - Ownership stake for which shareholders are responsible.
  - If liabilities outweigh assets, shareholders are accountable for the extended liability.
  - If assets exceed liabilities, shareholders have positive equity.

- Assets = cash, inventory, accounts receivable (amount due by customers), property and equipment, prepaid accounts, accumulated depreciation.
- Liabilities = accounts payable (money owed), interest payable, leases, current long-term debt (amount of principle paid for the period), long-term debt (amount still owed by company).
- Current Accounts = assets and liabilities that can be converted quickly.
- Current assets = considered cash equivalents on the balance sheet,

- shareholder equity can be increased by using profit to pay down debt.

<u>Cash Flow Statement</u>

- how cash inflows and outflows affect an organization.
- whether the organization is generating enough cash to cover operations and acquire additional assets.

- <u>Net Operating Cash Flow</u> – amount of cash generated (or consumed) through company operations.
- <u>Net Investing Cash Flow</u> – amount of cash generated (or consumed) by investing in other organizations or selling or acquiring buildings or property.
- <u>Financing Cash Flow</u> – cash generated by obtaining loans or other financing.

Financial Analysis

- financial decisions are based on past performance and projected future performance.
- To determine whether the financial return is worth the expected risk.

<u>Profitability Ratios</u> – organization's ability to generate income beyond expenses.

<u>Profit Margins</u> - reflect a company's profitability.

- <u>Gross profit margin</u> – based strictly on sales and costs of goods sold.
- <u>Operating margin</u> - earnings before EBITA.
- <u>Net profit margin</u> – net profit after all expenses are included.

<u>Returns</u> – demonstrates how well a firm has done in making money.

- <u>Return on Assets (ROA)</u> – ability to generate income based on assets, independent of financing.
- <u>Return on Equity (ROE)</u> – using financed assets to generate income.
  - <u>Leveraging</u> – borrowing capital to purchase assets.
  - <u>ROE</u> – measures effectiveness at using loans to generate profit.

<u>Earnings</u>:

- <u>Earning per Share (EPS)</u> – income (or loss) generated per share.
- <u>Price to Earnings (P/E)</u> – company's share price related to its EPS.
  - Whether an organization is fairly valued.
- General benchmark is 17.

Risk Ratios – risk an organization faces in its operations.

- the analysis focuses on whether a company will have the ability to cover expenses and operating costs.
- Current ratio – ability to cover short-term obligations.
- Quick ratio – ability to cover liabilities with current assets than can be quickly converted to cash.
    - also known as the “acid test”.
    - More accurate picture of an organization’s ability to cover bills.
- Debt to equity ratio – analyzes how a company funds its growth and operations.
    - Highly leveraged - may reduce profits due to interest expenses.

Limitations of Financial Statement Analysis

- does not directly consider changes in market conditions.
- Declines in margin may be a result of poor economic conditions rather than poor company operations.
- SOX established the Public Company Accounting Oversight Board,
    - Monitors the independent auditing of publicly traded companies.

Budgets

- process for planning where money is to be allocated for the year.
- Financial tool that estimates costs and revenue and provides a variance warning mechanism and fiscal uniformity for the company.
- Top-down approach – management allocates a specific amount of money to the security department without input from the security department.
- Bottom-up is when front line managers set their own budget.
- (Combination of both is best practical solution).
- Budgets are politically charged because the amount of capital is limited.
- Effective tool for allocating funds to Bus based on expected revenue.
- Line items – specific entries with predetermined limits.
- Sometimes spending beyond is necessary to take advantage of opportunities.
- Benefit of the investment divided by the cost – calculates the ROI against the expense.

Return on Investment

- effective way to compare the desirability of different ways of spending.
    - ie. Paying down debt is like an investment, and the interest avoided is like revenue.
- Return on Implementation – measured by applying an efficiency vs. cost, or cost vs. benefit. (ie. Lower insurance premiums).

Jonathan Taormina, CPP, CFE, PCI

CHAPTER 3 STANDARDS IN SECURITY

- criteria, guidelines, and best practices.
- More than 95,000 standards – recognized in the United States.
- Security arena – consensus, openness, due process, transparency.
- A standard is **voluntary** – different from a regulation. (Though some regulations may require compliance with a standard).
- Best practices, lessons learned, define measurement methods, document equipment performance, establish design requirements, consistency of services.
- Cross-jurisdictional information sharing.
- Interoperability (ie. Communication protocols).
- "When standards work, you don't notice them, you take them for granted".
- Developed on national, regional, and international levels.
- Many players involved:
    - National Fire Prevention Association (NFPA) has issued several standards related to security.
    - American National Standards Institute (ANSI).
    - International Organization for Standardization (ISO) – world's largest.
- Standards determined by need.
- Broad Stakeholder participation – all interested parties.

International Organization for Standardization

- world's largest.
- Greek word *isos*, meaning equal.
- Nongovernmental organization.
- Each member country has one vote.
- Decided by consensus – not majority vote.
- Voluntary – Conformity NOT compliance.
- Worldwide applicability.
- Technical committees – ensure that a standard is relevant, credible, and broadly acceptable.
- National mirror committees – technical advisory group of subject experts and interested parties. Convenient for thos unwilling or unable to travel internationally. Main responsibility is to develop a national consensus to present to ISO
- Liaisons and Observers Do NOT vote.

American National Standards Institute (ANSI)

- formed in 1916 as a clearinghouse for Standards Developing Organizations (SDOs) in the United States.
- SDOs develop standards within there area of expertise.
- Voluntary.
- Market driven, flexible, sector based – led by the private sector and supported by the US Government.
- Standards users, not standards bodies – drive standardization activities.

- ANSI accreditation – signifies procedures sponsored by an SDO satisfy ANSI requirements.
- ANSI accreditation is a precondition for submitting a standard for approval.
- Approval is subject to ANSI procedural oversight, due process and audit.
- Consensus.
- Public review.
- Compliance is not mandatory unless adopted into a statute or regulation.

Management Systems Standards

Management System – organization's method of managing its processes, functions, or activities.

- developed to be generic.
- Framework – leaves discretion.
- Conformity gives customers a greater confidence in its reliability.
- Standards are tools – NOT regulations.
- Based of the Plan-Do-Check-Act (PDCA or Deming Cycle) model of Total Quality Management (TQM).
- Holistic, strategic approach to management.
- Organization has flexibility.
- Can confirm in whole or in parts of the organization.
- Requires engaging top management.
- "Management speak" – using the same language as top management.
- Benefits:
    - Establishes benchmarks, identifies risks and potential solutions, includes all levels of employees and stakeholders in planning. Enhances performance, protects reputation, ongoing system of continual improvement.
    - Checked not for specific performance but for a mechanism for improving performance.

Plan-Do-Check-Act (PDCA) cycle

- structured problem solving focused on continual improvement.
    - Plan – most critical stage.
    - Do – detailed action plan.
    - Check – are the solutions producing outcomes.
    - Act – if so, standardize the solutions throughout the organization.
- Pick a solvable problem and practice using the management system.

Well-Known Management Systems Standards

- ISO 9000	Quality management.
- ISO 14000	Environmental management.

ASIS Global Standards Initiative (GSI)

- started in 2007.
- Liaison – ASIS is not a country and therefore cannot participate directly in ISO as a national member.
- ASIS is also an ANSI accredited SDO.
- ASIS promulgated several **guidelines** (less formal than standards).
- ANSI BSR8 form submitted for 45 day Public review.

  (several guidelines and standards are listed on pages 50-53)

- Security in the ISO context is very inclusive:
  - Prevention, preparedness, mitigation, response, continuity, and recovery.
  - Example: ANSI Standards Boost Business (SBB) campaign:
    - Effort to increase c-level understanding of how voluntary standards can boost business performance.
- US Department of Defense reached out to ASIS to develop standards for the private security force.

Organizational Resilience Standard

- developed by technical committees.
- Managing the risk of a disruptive incident by addressing reduction of both likelihood and consequences.
- Know the organization:
  - Critical objectives, operation, functions, products/services.
  - Prioritize them.
  - Approached from a business point of view.
- Security policy – obtain management commitment.
- Planning – risk assessment and impact analysis.
  - ISO31000:2009 – Risk Management Guidelines.
  - Prevention, response, reducing impact, returning to normal ops.
- Implementation and Operation – improving resiliency.
  - Strategic plan, training and awareness, communication, documentation, and incident preparedness and response plans.
- Checking and Corrective action.
- Management review:
  - Repeat previous steps.
  - Ownership throughout the organization is key to success.
- If the people who will use the standards get involved in developing them, the standards are more likely to be useful tools.

Jonathan Taormina, CPP, CFE, PCI

CHAPTER 4 INTRODUCTION TO ASSETS PROTECTION

Assets – people, property, and information.
Intangible Assets – reputation, relationships, and creditworthiness.

Effective Defense-in-Depth asset protection program
The greatest protection of corporate assets occurs when an appropriate mix of physical, procedural, and electronic security measures is in place in relation to the assets being protected.

Proactive function directly tied to organization's mission.

Tangible assets – can be seen, touched, and directly measured.
Mixed assets – tangible and intangible.

Assets Protection incorporates:

- all security functions and investigations, risk management, safety, quality/product assurance, compliance, and emergency management.

Countermeasures – include people, hardware, and software.

Convergence – integration of traditional and information systems security functions.

Most US critical infrastructure is owned or operated by private enterprises.

9/11 changed expectations and the level of security the public will tolerate.

Risk Management

- asset protection is increasingly based on the principle of risk management.
- Risk – the possibility of loss resulting from a threat, security incident, or event.
- Asset protection's primary objective is to manage risks by balancing the costs and benefits of protection measures.

Current Practice of Asset Protection

Five avenues to address risk

- Avoidance
- Transfer
- Spreading
- Reduction
- Acceptance

Balancing Security and Legal Considerations – the right balance is needed.

Jonathan Taormina, CPP, CFE, PCI

The 5 D's

1. Deter.
2. Deny (the adversary access).
3. Detect.
4. Delay.
5. Destroy (the aggressor).

Health Care Sector

- patients are vulnerable.
- HIPAA regulations.
- Sensitive information, intellectual property, facilities, materials.

Educational Sector

- assaults against students, theft, vandalism.
- Crisis management (ie. Community shelters).
- Foreign student behavior.
- Reputation of university.
- Gangs, alcohol/drugs.
- Inappropriate teacher/student relationships.

Fast Food Sector

- quick-service restaurants (QSR).
- Theft, fraud, point of sale systems.
- Supplier/vendor integrity.
- False claims of employee or customer injuries.

Telecommunications Sector

- designation as national critical infrastructure.
- Information security, network and computer security, fraud prevention, physical security.
- Affected by government regulation – mandated security practices.
- Electronic signals – susceptible to physical and electronic threats.
- Property rights and access issues (ie. TWC).

Aerospace Sector

- sensitive information, classified information, regulatory and reporting compliance, travel security, test and evaluation program security.

Forces Shaping Assets Protection

Technology and Touch

- balance between human and technological solutions.
- “high-tech intoxication”.
- We look for the quick fix – implemented haphazardly.
- We fear and worship technology.
- We blur the distinction between real and fake (ie. TV and video games), causes a delay in reaction, we accept violence as normal.
- We love technology as a toy – expensive if no real need.
- We live our lives distanced and distracted
- Crime Prevention Through Environmental Design (CPTED)
    - psychology, architecture, and other measures.

Globalization in Business

- brings threats closer and may increase vulnerabilities.
- Vulnerabilities presented by political and economic openness.
- Major business functions are outsourced.

Standards and Regulations

- Voluntary standards – ISO, ANSI, NFPA, UL.

Statutory or Regulatory Standards

- binding under the law and enforced by formal authorities.
- ie. International Maritime Organization (IMO).

Mixed Standards

- technically voluntary but practically obligatory.
- May determine the availability and cost of casualty insurance.

Professional Certifications and Licensing

- ASIS, International Foundation for Protection Officers, ISC2 International Information Systems Security Certification Consortium.
- Some jurisdictions require licensing for security practitioners.

Convergence of Security Solutions

- integration of traditional and IT security.
- Information security, personnel security, technical security, public relations, security architecture, CPTED, investigations, policies, and awareness training.

Homeland Security and the International Security Environment

- there is a danger in overemphasizing the threat of terrorism and not addressing the broader security issues relevant to a particular environment.

Jonathan Taormina, CPP, CFE, PCI

Management of Assets Protection

Technical expertise ----- Management ability ----- Ability to deal with people.

Concepts in Organizational Management

Planning Organizing Directing Coordinating Controlling

- Who is the customer? – define business purpose and mission.
  - Many organizations serve multiple customers.
  - Commitment to business mission, not just security.
- Quality – belongs to everyone, all the time.
  - Conformance to customer requirements.
  - Quality should be cultural and integrated into all business practices.

Management Applications in Assets Protection

- Planning – developing strategic goals and objectives.
- Management – conducting day-to-day operations.
- Evaluation – assess how well objectives are being met.

Span of Control – a single person can supervise a limited number of staff

- general rule is 1:10.
- Settings that emphasize self-directed, cross-functional teams and very flat structures, span of control is less relevant.

Unity of Command – an individual reports to only one supervisor.

Behavioral Issues in Assets Protection

- behavioral science is the study of people and their relationships to each other.

Maslow's Hierarchy of Needs

- behavior is driven by basic needs at different levels.
- Self-actualization is highest (realizing one's full potential).

McGregor's Theory X and Theory Y

- Theory X – workers are lazy and tend to avoid work.
- Theory Y – workers are naturally motivated and want to work hard.
  (Programs based on Theory Y are more successful)

Herzberg's Motivation-Hygiene Theory

- the opposite of satisfaction is not dissatisfaction but simply no satisfaction.
- Motivators – achievement, recognition, responsibility, satisfaction from the work itself.
- Hygienes – surroundings, conditions, salary, coworkers, and other external factors.
  (only motivation factors can move a person from no satisfaction to satisfaction). Hygiene factors may alleviate dissatisfaction but will not result in satisfaction. No quick fixes.

Applications of Behavioral Studies in Assets Protection

Crime Prevention and Reaction

Private security – prevention of crime.
Law Enforcement – crime control.

Incident management – how people will react

Security Personnel Management – what motivates/demotivates people.

Employee Training and Awareness

- when a subordinate requests advice, avoid giving a specific solution….. guide the subordinate through an open exchange of information.

Liaison and leveraging other organizations

- inside and outside the organization….collaboration.

Insurance as a Risk Management Tool

- best known form of Risk Transfer.
- Proactive – asset of the organization.
- Reactive – only used after a loss occurs.
- Indemnification/compensation.
- Specified losses from specified perils.
- Two categories: Property and Liability.
- Contracts are seldom read until after a loss.

Peril – the cause of the possible loss.

- named perils contracts – specifies covered perils.
- All risk contracts – covers all perils except those specifically excluded.

Burglary/Robbery in insurance terms:

- Burglary – gaining entry to premises by force.
    - there MUST be physical marks.
- Robbery – forcible taking of property (used or threatened).
- if no visible marks or force:
    - theft or larceny policy is required to be covered.

Defining the property covered

- does not cover every property owned – property exclusions.

Defining the losses covered

1. direct loss.
2. Loss of use.
3. Extra-expense losses – ie. Defending a liability suit and paying a judgement.

- Most policies cover direct losses only.
- Actual cash value – cost to replace/restore, less depreciation.

Defining the Period of Coverage

Occurrence loss – loss occurred during the period the policy was in force no matter when the occurrence was discovered.

Claims-made – coverage only for losses reported during the period the policy is in force.

Tail cover – coverage for events that occurred during a prior policy period but are raised during the tail period. To change carriers, it is normally necessary to purchase tail cover from the prior carrier.

Defining the People Covered

- many property policies allow space for indicating the name of the lender.
- Frequent technique to extend coverage is to have an individual designated as a named insured in the policy.

Defining the Time of Coverage

- some start at noon, standard time; some start at 12:01 am.

Conditions that Suspend Coverage (Exclusions)

- endorsements, which might result in increased premiums.
- “while” or “if” clauses:
  - suspended while certain conditions exist.
  - Suspended if defined conditions exist.
- Vacancy clause – suspends coverage while a property stands vacant beyond a specified period.

Endorsements

- standards policies may be modified by endorsements ---- riders.

Crime Coverage

- two types of bonds may be issued for protection:
  - Fidelity – for dishonesty of employees.
  - Surety – guarantees credit or performance by an individual.
- Comprehensive 3D policy is a combination fidelity crime insurance policy designed to offer the widest possible protection.
- Consider an endorsement for IT equipment and data.
  - Loss of data or reconstruction of data.

Business Interruption

- resulting in financial loss.
- Endorsements known as contingent business interruption loss forms.
- Endorsement extending the period of indemnity – if a business may not return to normal for some time after reopening following a shutdown.
- Valuation
  - Actual loss sustained – must prove the claim.
  - Valued-loss method – specific amount ($) payable each day for a specified period of time.
  - Business interruption and extra expense endorsement (ie. Keeping a product on the market regardless of expense).

Liability Endorsements

- under Tort law – entitled to collect for losses and mental anguish from anyone they can prove responsible for intentionally or negligently injuring them or damaging their property.
- Commercial general liability policy – less comprehensive than assumed.
  - Several endorsements should be added.

Liability of Officers and Directors

- "while acting in the scope of their duties".
- "while acting in behalf" of the enterprise. (more inclusive).

Employee Practices Liability Insurance (EPLI)

- work related lawsuits (ie. Harassment, wrongful termination, etc.).
- covers defense costs, judgments and settlements, BUT may not cover punitive damages, fines or penalties.

Product Liability

- used by manufacturers and dealers of goods.
- Based on either the tort theory of negligence or the contract theory of breach of warranty.
- Product recall – can be added as an endorsement.
  - This is called product recall or product withdrawal expense.
  - The loss of the product itself is NOT covered.

Insurance Providers

- financial stability and claims settlement history is critical to timely reimbursement.
- Can be bought directly from insurance company or a broker.
- Captive carrier – buying the insurance company.
- Mutual insurance organizations – Risk retention groups.

Insurance Companies

- choosing the wrong company can, in itself, be a high risk.
- Annual reviews.
- Ratings of insurance carriers measure the financial condition but NOT the speed of claims payments.

Insurance Brokers

- marketing specialists who deal with agents or companies.
- Broker who arranges insurance coverage with an insurance company that becomes insolvent may become a defendant in a civil action.

Risk Retention Groups (RRGs)

- corporate bodies authorized under some state laws as liability insurance companies.
- Market their liability policies to purchasing groups (PGs).

Captive Carriers

- a separate, wholly owned or principally owned firm, usually organized offshore, used to write the insurance for the owning company.
- Makes it easier to insure risks not acceptable to conventional carriers.
- Generally a technique of larger firms.

CHAPTER 5 COST-EFFECTIVENESS AND LOSS REPORTING

Standard Management Practices

- return on investment strategies, metrics management, data capture and analysis, and cost benefit analysis.

Cost Effectiveness

- producing good results for the money spent.
- Measureable in financial terms.
- Some elements of the security program may take several years to implement.
- Procedural controls are the least expensive countermeasures.
- Does the assets protection program accomplish anything that can be quantified and that justifies its cost?
- Cost must be weighed against the consequences of not having a security program.
- Main expense categories: salaries, operational expenses, and capital expenditures.

Return on Investment (ROI)

- ROI is a standard profitability ratio that measures how much net income the business earns from each dollar invested by its owners.
- Gauges management's overall effectiveness in generating profits.
  - $$\frac{AL + R}{CSP} = ROI$$

- AL = avoided loss.
- R = recoveries made.
- CSP = Cost of security program, including personnel, admin, and capital costs.

Security Metrics

- process of measuring an asset protection program's costs and benefits as well as its successes and failures.
- Perform an analysis of potential areas of loss, their probability, and the impact on the corporation.
- Metrics can show cost effectiveness.
- Data analysis may also suggest whether specific security measures are effective at all.

Budget Process

- determine the profit the business must earn and subtract that amount from estimated revenues. This leaves the amount available to run the business.
- Must demonstrate that the real costs to the enterprise would be greater if the level of support for the program was reduced.

Cost Reduction

- examined for cost effectiveness.
- Periodic examination – not “the way we’ve always done it”.

Cost Avoidance

- avoiding costs or expenses through the use of asset protection resources.
- ie. A security officer taking corrective action while on patrol (such as turning off lights).

Other Strategies

WAECUP –	Waste, accidents, error, crime, unethical practices.
SWOT –	Strengths, weaknesses, opportunities, threats.
STEP –	Social, technological, environmental, and political.

Data Capture

- collecting information.
- Design a good report form, teach security how to use it, prompltly collect and analyze, produce management reports.
- Management reports should show individual and cumulative costs that were avoided.

Data Analysis and Display

- software must aggregate the data for analysis.
- Trends, successes, failures, costs, losses, savings, what works and what doesn’t work.
- Use graphical displays for upper management decision makers.

Claims Avoided

- workers’ compensation, disability, accident, and health issues.
- Investigations could find fraud on the part of the claimant.

Proofs of Loss

- insurance companies typically require proof of loss before making payments.
- **Losses caused by outsiders has a much larger deductible than its insurance for insider theft (fidelity coverage).**
- Might want to prove it was an insider:
    - Outsider could not have gained access.
- Include labor costs elements if components had been worked on by the enterprise.
- Net amount of the claim can be added to the security database for later reporting.

Recovered Physical Assets

- cost of the item recovered PLUS the cost of replacement.

Uninsured Claims or Causes of Action

- a security investigation often leads to a formal statement.
- May lead to actionable claims by the enterprise for financial recovery instead of an insurance claim.

Other Actions

- matter is handled by security instead of a collection agency which gets a percentage of the recovery.

Systematic Incident Reporting

- track and analyze.
- History of events.
- A Statement of Enterprise Policy is needed.
- Incident profiles.
- Modus Operandi files to assist in countermeasures or recovery efforts.
- Asset description and valuation.
- Total number of incidents is used to establish criticality of exposure.
- Frequency of incidents determines probability.

Creating an Incident Database

- from which to extract information.
- If no central database – incidents are seen as unique events.

Functions of an Incident Report

- data on which to base security functions.
- Identifies if no accountability control exists.
- Identifies items targeted.
- Whether countermeasures were effective or not.
- Plot event trends.

Policy on Submission of Incident Reports

- employee notifies immediate supervisor.
- Supervisor prepares reports and submits to security.

Incident Database

- converted to a computer file.
- Management reporting periodically to upper management.
- Modus Operandi – security should develop information even if another department manages the files.
- Corrective Action Report – by unit responsible for the incidents, and total loss charged to that unit.
    - Alerts units for immediate corrective management action.
- Loss Status Report – distributed to senior management.

Jonathan Taormina, CPP, CFE, PCI

Predictive Modeling by the Security Organization

- avoiding future incidents through planning.
- Most vulnerable, time, locations, countermeasures, slips and falls, health and safety, and other incident that costs money.
- The selection of countermeasures depends on the return on investment.

Protection Planning Without an Incident Database

- form an asset protection committee.
- Determine criteria and identify vulnerable items.
- Develop a system for tracking.
- Assess vulnerability.
- Select countermeasures.
- Cost benefit model – countermeasures can be justified.

Pilot Verifications of the Model

- select some points of exposure and provide countermeasures, while leaving others unprotected. Compare the results and adjust accordingly.

Modifications of a Growing Database

- security management review the data periodically.

Basis of valuation

a. purchase price.	3750.00	
b. Book value.		
c. Replacement cost	10,000.00	total cost 13, 750.00
d. Other		

Notes on History Reporting Form

- creating a document history helps in tracking changes made to the document.

- security loss/incident report shall be submitted for each case.

CHAPTER 6 THEFT AND FRAUD PREVENTION IN THE WORKPLACE

Theft - dishonest appropriation of property belonging to another with the intention of permanently depriving the owner.

Fraud - intentional deception perpetrated for the purpose of unlawfully taking another's property – theft by deception.
(victims have at their disposal – criminal and civil remedies).

- Theft and Fraud are most frequent and costly forms of dishonest.
- Motive, ability, opportunity.
- An organization's greatest threat, second only to competition.
- Most cost effective way to deal with fraud is to PREVENT it.
- Median recovery for losses was only 20% of original loss.
- 30% of business failures result from employee theft.
- Most perpetrators are first time offenders.
- 6% of annual revenue is lost to fraud.
- 2 million shoplifting arrests each year.
- Employees steal over a billion dollars a week.
- Will steal to the extent the organization will allow.
- Prevention tool to reduce the level of employee theft is a climate of trust, honesty, and cooperation throughout the workforce.
- Fraud, in a sense, is a TAX.
- Loss should be measured by extrapolating the amount of sales and other costs such as downtime and insurance rate changes necessary to cover the loss.
- Serious form of embezzlement is fraudulent cash disbursements.
- Time theft is every employer's nemesis.
- Perpetrated by employees with access.
- Lack of supervision and effective processes are the primary contributors.
- 5% of employees responsible for 95% of workplace theft.
- More fraud is revealed by employee tips than any other formal internal processes.

Retail Industry

- 70% of losses = employee theft
- employee theft is $15 to every $1 of shoplifting.

Employee Theft

- Social Control - more likely to steal if they perceive little threat of detection or punishment.
- Youth and external pressures do not always account for the reasons.
- Opportunity and job dissatisfaction.
- Theft of time - extended breaks, sick time, improper timecard punches.

Prevalence of Employee Theft

- 1/3 of employees reported stealing.
- Vast majority take small amounts.
- Diversion, conversion, disguise, divergence.
- Few people steal company property to ease economic pressures.
- Majority of large scale thefts – committed by managers.
    - Embezzlement – by a person to whom it was entrusted.
    - Defalcation – money held in a fiduciary capacity.
- Youth reported more deviance than older workers.
    - Least committed to the organization – less invested.

Job Dissatisfaction and Effects of Social Control

- retail employees with greatest access to cash and high-value merchandise are most likely to steal.
- Employees with the greatest access.
- Hospitals – nursing staff.
- Employees are greatly influenced by informal social controls.
- Job dissatisfaction and theft are correlated.

Fraud and Related Crimes

Differential Association Theory (Edwin Sutherland)

- criminal behavior is most often correlated with an individual's association with a criminal environment.

Non-shareable Needs Theory (Donald Cressey)

- defines the problem as a violation of a position of financial trust.
- Become trust violators when they visualize themselves as having non-shareable financial problems.

Common Elements of Fraud

- financial pressure, opportunity, justification (rationalization).
- Predominant factor is GREED.
- Absence or weakness of internal controls.

Employee Red Flags

- Situational – debts, credit ratings, alcohol/drugs, perceived inequities.
- Opprotunity – position of trust, knowledge of key operations.

Organizational Red Flags

- Situational – costs rising faster than profits (profit squeeze).
- Opportunity – abuse, and poor management of employees.

Sarbanes-Oxley Act (SOX)

- Public Company Accounting Reform and Investor Protection Act of 2002.
- Accounting scandals at public companies.
- Accounting scandals and business practices.
- CEOs must certify accuracy.
- Imposes civil and criminal penalties.

Scope of the Problem

Establishing a Prevention Program

- must move from reactive to proactive.
- Avoid ---- most companies resolve the incident and then slip back into a state of acceptance.
- Skimming – theft of cash, diverting cash "off the top".
- Lapping – taking small amounts from incoming invoice payments and then applying subsequent payment to cover the missing cash from the previous invoice, and so on…..
- Kiting – any fraud that involves drawing money from a bank account without sufficient funds to cover the check.
- Conversion – receiving of money/property and fraudulently withholding or applying it for one's own use.

10 Elements of a Comprehensive Model:

1. Prevention programs – process, policy, accountability systems, separation of duties, employee communications, prevention training, avenues for employees to report concerns, frequent audits.
2. Incident – quick and accurate reporting as soon as suspected.
3. Incident Reporting – encouraged to report. Culture of integrity and honesty.
4. Investigation – clear guidelines of what is expected to be accomplished.
5. Action – take immediate action.
6. Resolution – appropriate discipline ---- Obtain a recovery.
7. Analysis – how and why the loss occurred.
8. Publication – newsletters or bulletins to inform employees. (obtain advice of counsel before publicizing the results of an investigation)
9. Implementation of Controls – may prevent future thefts.
10. Compliance Testing and Training – periodic testing or auditing.

Dangers of Undetected Theft and Fraud

- organizations may become complacent.
- Over time, the negative variance may grow resulting in significant loss.
- Priority must be given to theft and fraud prevention.

Jonathan Taormina, CPP, CFE, PCI

50 Honest Truths About Employee Dishonesty
only some are listed here:

- employees can create an atmosphere for honesty or dishonesty.
- Theft is the ultimate sign of employee disrespect.
- Usually involved in prior misconduct.
- Employee who steals is more insidious than an outsider.
- Tenure is not an insurance against theft.
- Need and opportunity are critical elements.
- Ethical makeup will temper temptation.
- Rationalization.
- Belief that everyone steals.
- Employees who steal from you think you're responsible.
- A thief learns to lie before he learns to steal.
- No theft should be tolerated.
- Employees who know are as bad as the thief.
- Most employees mistake kindness for weakness.
- Most employees appreciate a second chance **– to steal from you again.**
- Be careful of the employee who discovered the loss.
- Better management could have prevented most theft.
- Cheaper to prevent it in the first place.
- Vigilance.
- Asset protection is everyone's job description.
- Asset protection is an insurance. The cost should be weighed against the risk.
- Deterrent effect of punishment is far shorter than you can imagine.
- The employee who says he's sorry usually is --- sorry to have been caught.
- Remorseful today will be spiteful tomorrow.
- If the employee offers to resign, accept it.
- Restitution does the victim the most good. More than termination or prosecution.

- private security operations.
- Includes critical infrastructures.
- Designed to supplement law enforcement agencies.
- Can be considered “para-police”.
- Security and public safety are not exclusive to government.
- Can be viewed as going back to the future (ie. 1800s).

<u>Historical Perspective</u>

- overriding human need = survival.
- The King’s Peace – equated to law and order.
    - Many offenses previously regarded as intentional torts, became crimes against the king’s peace.
- Law and order rested on the citizenry.
    - Hue and Cry was a call to order to all able bodied men.
- Similar to “observe and report” function of private security.
- Security officers should be a deterrent and immediately report crime to the public police.
- “Watch and Ward” = shire reeves (sheriffs) appointed by the king.
    - Similar to citizens hiring security firms within the public realm.

<u>Conceptual Perspectives</u>

- Private/Substitute cell – security provides the majority of security services.
- Public/Substitute cell – security personnel replace fired police.
- Private/Supplement and Public Supplement.
- <u>Public Supplement (focus of chapter):</u>
    - Likely to grow substantially.
    - Time share – provides patrol and other services to numerous clients, who each pay a proportionate share of the costs.
- <u>Public Safety Policing</u> – new policing model in which private security provides services within public areas.

<u>Public/Private Partnerships</u>

- Operation Cooperation – security and police work together to combat crime and deliver public safety services.
- ie. NYPD Shield.
- Structural and contractual enhanced coordination.
- Hallcrest Reports – sough to compare the U.S. security industry to public law enforcement quantitatively.
- **Some argue that private security is now the primary protective resource in the United States.**
- Not a loss of confidence in the police, but a desire to have more police.
- Today’s security industry is being compared to public policing in the mid-19th century.

Contemporary and Operational Issues

- cost is a significant distinction between public and private policing.
- Labor cost savings.
- Personnel expenditures are often the largest municipal budgetary line.
- Alarm response – 95% are false alarms.
- Almost 80% of police resources are used in "social worker" work.
- Only 20% is devoted to crime related matters.
- Instead of watching to prevent crime, motorized police patrols are usually waiting to respond.
- Security firms are more oriented towards pleasing their clients – by preventing problems, including crime.
- A proactive crime control strategy is costly and very labor-intensive.
- Community policing has created additional tasks.
    - Personnel and resources associated with the tasks.
- Supplement strength with private security personnel.
- Crime prevention and order maintenance = Private Security.
- Client service designed to prevent and control crime.
- Not "rent-a-cops" – but alternative service providers.
    - Lower cost – equated to outsourcing.
- Public police are over burdened with service oriented functions.
- 85% of all critical infrastructure in the U.S. – private security.
- Sustained with little or no municipal expenditure.
- If taxes are used – a special; taxing district is required.

Order Maintenance

- contends that crime problems originate in relatively harmless activities.
    - Public drinking, graffiti, loitering.
    - Disorder reduces social controls.
- Focus has shifted from socioeconomic factors toward physical characteristics (Environmental factors).
    - Situational crime prevention by assessing the circumstances surrounding the crime.
- Key to crime control = addressing both physical and social conditions.
- Order Maintenance:
    - Rehabilitation of physical structures, planting flowers, trees.
    - Look and feel of the area coupled with reducing or eliminating antisocial behaviors.
- Community Policing = fear reduction through order maintenance.
    - Reduce calls for service by addressing the underlying reasons.
- Private sector – focus on prevention.
- Tort claims on grounds of premises liability or negligent security.
    - Property owner knew or should have known.
    - Property owner motivated to institute security measures.
- Security seen as an asset and crime control as a duty.

Jonathan Taormina, CPP, CFE, PCI

Crime (fear of Crime) and Terrorism

- signs of criminal activity, such as disorder and incivility, have an impact on people's perception of crime.
- Incivility is equated with disorder; both represent chaotic conditions that result in more serious criminal activity.
- "Citizens are the law and order in a community, not the police".

Principles of Private Policing

- there is substantial evidence that labor costs have a direct relationship to service quality.
- Private firms have less constraint on process and more focus on results.
- The absence of market competition in the public sector allows for complacency.
- Private sector accountability and standards.

Policing Role and Functional Distinctions

- public police are sworn by government officials.
- Philosophical – may lack moral authority government can give.
- Legal – limited powers.
- Financial – can perform certain tasks more cheaply.
- Operational – more flexible.
- Security/political – private police give citizens more control.
- Community Policing model – the citizens are the clients.
- This seemingly private function provides an external benefit to the larger society.
- Knowledge of a client's interests affects how a security firm performs.
- Private police – delivery system is profit-oriented.
    - 30-day termination clause.
- Police Departments – less efficient; complacent.
- Constitutional protections – courts are now inclined to extend protections to cover actions by private security personnel.

Private Policing Environments

- additional layer of security for the community.
- Frees up public police for crime fighting.

Private: Supplement

- ie. Gated communities

Public: Replacement

- appearance of public police at a lower cost.
- Police replaced with private security firms.

Public: Supplement

- most common as a supplement, not replacement of public police.

1. Grand Central Partnership
    a. Each property owner is taxed.
    b. Security, sanitation, tour guides, lighting.
    c. Built on the logic of "order maintenance".
2. Metro Tech Area
    a. Security and sanitation.
    b. Order maintenance and citizen assistance.
3. Center City District
    a. Philadelphia BID
    b. Security and order maintenance approach.
    c. Public concierges and neighborhood watchers.
4. Downtown St. Louis
    a. Police and private entered into a supplemental, contracted relationship – private uniformed security patrol the central city.
    b. Same powers of arrest as police.
5. Greater Green Point Management District
    a. Houston, Texas
6. Durham, North Carolina
    a. Wackenhut Security patrol of buses.
    b. Same arrest powers as public police officers.
7. Dallas Downtown Improvement District
    a. Order maintenance approach
8. ***Starrett City:***
    a. Classic model of the benefits of privatization.
    b. Special police designation – full arrest powers.
    c. Only physical distinction is the private security personnel.
9. San Francisco Patrol Special Police
    a. Owners of certain beats or territories which can be sold if approved by the police commission.
10. United Kingdom
    a. Guardforce Security Services.
11. Toronto, Canada
    a. Intelligarde – the law enforcement company.
    b. Clients are provided verification of time and location of patrols through GPS monitoring.
12. Marquette Park
    a. Southwest side of Chicago.
    b. Creation of special services districts – created by referendum.
    c. Sole service provider – intermediary between community and the security firm.

- Private police are public actors, and constitutional provisions are applicable to their actions.

Jonathan Taormina, CPP, CFE, PCI

The Future of Private Policing

New Policing Model

- Can municipal police departments perform as first responders for homeland security and at the same time operate with a community service orientation?
- What future role will alternative service providers have in the delivery of public safety services?

- Private police- excellent providers of community policing because of their responsiveness to their clients.
    - para-professionals of the police department.

Public Safety Policing Model

1. Tactical operations – SWAT, gang/drug units, saturation units.
2. Tehnological functions – networked cameras and access control.
3. Order maintenance – control the environment.
    a. Focus on physical aspects and social incivilities.

Legal/Licensing Standards

- recommended to be vested with some governmental authority.
- Private citizen Special Police Peace Officer
    - Peace officer arrest powers are available to the special police officer on duty only.
- Certain benefits by being "blessed" by government – moral and legal authority that most citizens respect.
- Special police designation may carry with it the protection of qualified immunity – a liability shield to protect the officer.
    - A liability shield is not applicable for reckless or malicious conduct but protects the officer who makes a mistake in behavior or judgment.
    - Reduces the legal exposure of the security firm and the insurance costs associated.
- Provides more professionalism in the security profession.
- Training and selection standards need not be equivalent to the public police:
    - Curriculum that focuses on the specific role or function performed.
- Assess both the function and criticality of the job.
    - Trained and licensed at different levels.
- Accountability – to the community, the law, and the larger society.
    - 1. Specific operating procedures.
    - 2. Community-based board to oversee the operations.
    - 3. Well-defined process for addressing complaints.
        - Separate board with subpoena powers, ability to conduct hearings, the legal authority for warnings, fines, and other employment remedies.

What was once a professional relationship between the public and private sectors has now become a professional **necessity**.

CHAPTER 8 CONSULTANTS AS A PROTECTION RESOURCE

- professional expert advice or guidance.
- Companies without a formal security function.
- Specific security related tasks.
- Desire for an independent, objective assessment.
    - Independent consultants – do not sell products.
- Often less expensive than hiring additional staff.
- Common concerns re: using consultants:
    - Security will look incompetent.
    - A negative report may reflect unfavorably on security.

3 Major categories:

1. Security management consultants.
2. Technical security consultants.
3. Security Forensic consultants.

Security Management Consultants

- largest group within this niche profession.
- Managing the protection strategies for the business.
- Targeted focus = Scope of Work.
- Will not get into technical specifics:
    - Functional concepts of a security system only.

Technical Security Consultants

- technical expertise.
- Translate concepts/functionality into detailed blueprints and equipment specifications.
- Work with architects and design engineers.
    - Eliminates retrofitting after it's built.

Forensic Security Consultants

- Investigation, identification, and collection of evidence.
- Identification of vulnerabilities, mitigation strategies, litigation.
- Expert witness on security related issues.

Security Advisory Committee

- internal resource.
- Critically examine the program, general oversight, assist in meeting corporate and government requirements.
- Chaired by a project coordinator.
    - Reviews the program at least quarterly.
- Members should represent key corporate functions.

Jonathan Taormina, CPP, CFE, PCI

How to Use a Consultant

- typically driven by a specific problem, need, challenge, or goal.
- Crime Analysis:
  - Penetrated preventative measures, frequency, temporal (time/day) details, risk, preventative measures.
- Mix of security solutions:
  - CPTED (environmental), policies/procedures, personnel, upgrading the physical security.
- Fresh set of eyes.
- Experience from other companies – Industry norms.
- Above company politics.

How to Find a Security Consultant

- be cautious of consultant claiming to address all issues of security.
- Referral from a colleague.
- International Association of Professional Security Consultants.
- ASIS.
- Institute of Management Consultants.
- Industry specific associations (ie. Buildings, hospitals, etc).

Selecting a Security Consultant

- FIRST: Define the Scope of Work.
- Develop a custom application that can be used to compare consultants.
  - Request both: Application and C/V. (may discourage weak applicants).
- Top 2 candidates – request redacted work samples.
- Provide a brief tour of facility.
- Begin negotiations with the top candidate.

Consulting Fees and Expenses

- There are no bargains – time and quality must be considered.
- Caveat emptor re: bargains.
- Consultants should track expenses using software (ie. QuickBooks).
- Hourly fees, daily fees, fixed fees, not-to-exceed fees, retainers.
  - Hourly fees – unusual in security consulting EXCEPT forensic consultants.
  - Daily Fees – multiply hourly rate x 8.
  - Fixed Fees – estimate of total amount to deliver the end product.
    - Not recommended as it might reduce the quality if the consultant has to eat unexpected costs/expertise.
  - Not-to-Exceed Fees – limited to agreed amount.
  - Retainers – services provided at a substantially discounted rate.
    - Paid even if minimum days are not used.
  - Miscellaneous arrangements – ie. Taking equity in client's business.
- Expenses:
  - Usually reimbursed at actual costs.
  - Should be same amount given to client's senior management.

Working with Consultants

- A Consulting Project Coordinator (often a member of the Security Advisory Committee) should be assigned.
- Outline the Scope of Work:
    - Work plan, progress reports, and Final Report.
- Project Coordinator (CSO or Security VP) – works closely with consultant WITHOUT any other management involvement.
    - Liaison between consultant and the company.
- Project Sponsor – possibly the person who suggested the project.

Organizational Orientation

- arrange an orientation for the consultant.
    - Organizational chart/Background data.
- Include results of previous projects.
- Identify cultural idiosyncrasies.

Levels of Assistance

- consultants are often given access to sensitive information:
    - Non-Disclosure agreement is necessary.
    - Method for handling of sensitive information.
- Conclusions/Recommendations – safeguarded by a limited number of individuals.
- Reports are subject to discovery by an adverse party.
- Methodology – industry guidelines:
    - ASIS *General Security Risk Assessment Guideline.*

Scope of Work

- Scope and objective of the project – should be part of the initial request for quote and included in written contract.
- Scope of Work – central objective, clear focus of the effort.
- Initial project review – should address strategies that will achieve the objective.
- Scope Creep – scope of work grows after contract has been signed and work begun. Both parties should agree to it in writing.

Work Plans

- tasks and priorities determined, assignments made, and completion schedules established:
    - Deadlines should be converted to Milestone Charts.
- Frequent progress meetings.
- Earned Value Analysis – measurement of project's progress.
- Project Coordinator – ensures deadlines are met and project is on schedule.

Progress Reports

- "if deemed necessary".
- Minutes of meetings outlining decisions made.
- Frequency depends on size and complexity of the project.
    - May forego interim reports.

Final Reports - recommendations and advice.

- Executive Summary.
- Results achieved.
- Define any additional work that needs to be done.
- Final briefing for top management.
- Recommendations should be numbered and the project is numbered the same as the recommendation (ie. Recommendation 23 – Project 23).
- Additional assistance identified:
    - Additional contract and new scope of work.
- Consultant may search for and pre-qualify a security executive to implement and manage the recommended program.
    - Fee is usually 25-30% of annual salary plus expenses.

Future of Consulting

- as companies downsize – frequently lose in-house specialists.
- Fees – many consultants are moving to project-based pricing.
    - Allows for budgeting a Closed-End cost.
- Consulting alliances – teamed with other consultants.
    - ie. Strategic partnerships.

Consulting applications should include copies of:

- professional indemnity (or equivalent) insurance certificates.
- Copies of liability insurance certificates (or equivalent).

In Agreement:

- "Consultant will disclose promptly to Company all ideas, inventions, discoveries, and improvements, hereinafter referred to as 'SUBJECT INVENTIONS'".
- All writings produced shall be the sole property of the Company.
- If consultant must store classified material offsite (ie DOD) – a facility clearance will be required.

Professional Services Log - maintained for 3 years.

Jonathan Taormina, CPP, CFE, PCI

CHAPTER 9 EXECUTIVE PROTECTION IN THE CORPORATE ENVIRONMENT

History

- Praetorian Guard – for Roman generals in the 2nd c.
  - Evolved to protect and appoint Emperors.
  - Disbanded – considered a disruptive force.
- Yeomen Guard – 1485, ruler of England.
- Modern history – Secret Service – 1865
- Coroporate sector – mid 20th c.
  - Workplace violence, kidnappings.
  - Potential for stock volatility.

Research on Executive Protection

- secrecy is often a condition of kidnap and ransom policies.
- Mental illness rarely plays a key role.
- Actual threats often don't make threats.
  - Identify, investigate, assess anyone whose behavior suggests a possible threat.
- Combination of Motives.
- Notoriety, fame, attention, avenge, to be killed, to save country, money, political change, or a special relationship with the target.
- Inappropriate or unusual interest coupled with some actions.

Basics of Executive Protection

- Business risk – executive is a valuable corporate asset.
- Stock price may slide.
- Executive's services will be lost.
- Employees may be distracted.
- If driven: executive can work from car.

Philosophy of Protection

- establish a crisis management team during the preplanning stage.
- EP specialist – bodyguard is not a favored term.
- Draw little attention.
- Prevent and avoid trouble – not combat it.
- Anyone can protect anyone.
- Brains not technology.
- Security vs. Convenience continuum.

Prevent and Avoid Danger

- anticipate threats.
- ie. Select hotels that are safe a plan fire escape routes.
- Anyone can protect anyone – it's a brain game.
  - Intelligent, trained, and physically fit.
- Don't stop to think – practice reactions to different scenarios.
  - "what ifs?"

- Keep Clients Out of Trouble
  - avoid dangerous persons/conditions.
  - Move principal out of harm's way.
  - Communicate subtly – nondescript phrases or visual cues.
- Security vs. Convenience Continuum:
  - As one increases, the other decreases.
  - Neither extreme is practical.
- Rely on brains not technology.
  - Technology may put subject in a vault.
  - Buy defensive time with equipment and remove principal.
  - Cover and Evacuate.

EP Risk Assessment

- financial gain is only one of the many motives:
  - personal grievances, greed, political, etc.
- appropriate allocation is based on risk assessment.
  - Threats the executive faces.
  - Likelihood they could be carried out successfully.
- Relative risk rankings – low, moderate, high, critical.
- Performed on a recurring basis.

The Power of Information

- changes in: executive's status, new threat groups, exposure in media.
- How well executive is known to potential adversaries.
- Internet used by bad guys for information.
- Any media publicity about a person's wealth is harmful.

Office and Home

- traditional security measures.
- Rings of protection – outer perimeter and one our more inner perimeters.
- Safe room.
- Physical security tactics – perimeter, access control, lighting, CCTV, intrusion detection alarm systems.
- Home is a softer target.

The Advance

- researching any location/destination prior.
- Reduces exposure by smotthing logistics.

Local Travel

- security driver and EP specialist.
- Factory armored vehicle blend in.
  - Bullet resistant metal panels and glass, run-flat tires, anti-exploding fuel tank, steel reinforced bumper, dead bolts, dual battery system, inside/outside intercom, remote starter.

  - GPS, locking gas cap, protected exhaust pipe, electronic aid system (OnStar), alarm system, mobile phone.
- Call main security office when underway – coded language.
- Car is "sterile" only when locked away or watched.
- Alternate routes, safe havens, police, hospitals.

Long Distance Travel

- many risks
- is the trip necessary?
- Know before you go = Internet, professional country briefing, social customs.
- Advance mission – local L/E, embassy, consulate.
- Review security tips with executive.
- Appropriate health related items.
- Keep a low profile.
- Avoid western gathering places if Department of State designated high risk – churches, nightclubs, etc.
- Know how to get out.
- FBOs are not prime targets (consider fractional aircraft ownership).

Working the Principal

- the choreography to physically move about with the principal.
- Close-in, personal – don't look like a bodyguard. Stand close enough to protect, but not to have to be introduced.
- Relationship – EP specialist may have to give orders and advice regularly.

4 steps in the chain:

1. Arm's reach – immobilize him. Beyond that, mover to cover and evacuate.
2. Sound off – "gun to the right".
3. Cover – with your own body.
4. Evacuate – shield and remove the principal.

Protection Resources

- Law enforcement contacts – intelligence.
- News and Briefings.
- Networking – colleagues (re: hotels, airports, vendors, etc).

Future of Executive Protection

- Technological miniaturization and combination – ie. GPS on person.
- Up-to-date travel information.
- Information Sharing and Analysis Centers (ISACs) – share threat information.
- Improved training equipment.
- Protected vehicles – appear normal.
- Body armor – not always available privately.
- Balance between security and convenience.
- Protecting a key corporate asset – executive's life and well being.
- Convenient and comforting to the executive.

Jonathan Taormina, CPP, CFE, PCI

CHAPTER 10 SECURITY AWARENESS

- consciousness of an existing security program, its relevance, and the effect of one's behavior on reducing security risks.
- Continuing attitude – take specific actions in support of enterprise security.
- Conscious attention.
- Employees and non-employees – Force multiplier for the security program.
- "the security of an organization rests squarely on the practices of employees"

Levels of Awareness

<u>Executive Management</u>

- if they perceive expense with no compensating return – they may reduce/eliminate the security program funding.
- Convey – benefits and reasonableness of expenses to those benefits.
- Financial contribution to the bottom line.

<u>Middle Management</u>

- accountable for the success of their individual departments.
- If the program does not support the business goals, they may not support the program.

<u>First-Line Supervision</u>

- concerned with specific processes or activities.
- Security awareness focuses on how the program aids or detracts from specific performance objectives.
- Most employee complaints – first raised with the supervisor.

<u>Individual Employees</u>

- must be willing and interested, NOT coerced and pressured.
- If supervisors/managers disapprove – employees will not support it.

<u>Non-Employees</u>

- vendors, suppliers, customers, service personnel, government representatives, and members of the public.
    - ie. Suppliers given access to sensitive proprietary information.
- Brief explanation and possibly a Confidentiality Agreement.

Purposes of Security Awareness

1. Protect company assets – prime responsibility.
2. Understand the relationship between security and successful operations.
    a. Value and cost-effectiveness.
3. Identify obligations under the security program – periodic refreshers.
4. Recognize the connection between the security program objectives and selected security measures – appropriate and necessary.
5. Familiar with the sources of help for carrying out security responsibilities.
    a. Specifics of implementation.
6. Comply with statutory of common-law requirements for notice.
    a. Physical, verbal, and symbolic indicators.
    b. Trade secret – secret and valuable.
7. Comply with regulatory requirements – conveyed to employees and others.
8. Comply with contract obligations.
    a. Briefings and security education and training.
    b. Due notice to employees of the rules they must follow.
    c. Insurance contracts – some require specific procedures.
9. Comply with company policies and procedures.
    a. ie. “Clean desk” initiative.
10. Prepare the organization for emergencies – better prepared to respond.
11. Reduce organizational liability – show that the company is aware of security and makes an appropriate effort to provide a safe environment.
12. Communicate the value of the security department – valuable service.

Developing and Delivering a Security Awareness Program

- why it’s required, the value, employee responsibilities, reporting of violations, how to identify indicators of risk.
- Focus on generating support for the security program.

<u>Techniques, Materials, and Resources</u>

- Written material.
    - Can be incorporated into materials used by other departments.
    - Cups, pencils, rulers, key chains, etc.
    - Potential penalties for violating security rules.
- Audiovisual material – important not to post sensitive material where it is publicly accessible.
- Formal security briefings.
- Integration into enterprise line operations.
    - ie. Performance reviews, bonuses, job descriptions, etc.
- Inside experts – company training staff and communications staff.
- Outside experts – communications, advertising, public relations.

Obstacles to an Effective Awareness Program

- Low credibility of the security department.
    - ie. If security lacks understanding of company functions.
- Organizational culture – "how it's always been done" syndrome.
- Naivete – employees will always do the right thing to protect assets.
- Perception of a minimal threat – insignificant or unlikely to occur.
    - ie. No Soviet Union, but China, Cuba, Saudi Arabia, Korea.
- Departmental of employee indifference.
    - Employees may not see security as their work.
    - Undesirable extra work
- Lack of reporting capability – effective reporting system.
    - "Information collection is the basis of a security management plan".
    - Incident reporting system allows security to measure their department's effectiveness and to report back to senior management.

<u>Measuring the Program</u>

- Metrics – quantitative, statistical, and/or mathematical analysis.
    - Company losses before and after security awareness implemented.
    - Number of persons briefed.
    - Cost of briefings per employee.

Engaging Employees to Prevent Losses

- all employees are responsible for helping to protect organizational assets.
- Security manager must become familiar with all elements of the business.
- Reduce losses relating to contractual, statutory, regulatory, insurance, or other concerns.

<u>Positive Security Contacts</u>

- maximize the positive (helpful) contacts.
- Promote personal safety and security of employees and their families.
- Employees may suggest other programs they would like provided.

<u>Policies and Procedures</u>

- Policies establish rules; Procedures explain how to follow the rules.
- Good policies are not enough – continuous training required.
- <u>IT policies</u> – some choose not to cooperate:
    - <u>Uneducated users</u> – limited understanding of consequences.
    - <u>Arrogant users</u> – feel they don't have to comply.

Jonathan Taormina, CPP, CFE, PCI

CHAPTER 11 WORKPLACE SUBSTANCE ABUSE: PREVENTION AND INTERVENTION

Drugs of Abuse– chemical substance that alters the physical, behavioral, psychological, or emotional state of the user.

- Psychoactive – mind-altering. Targets the central nervous system.
- Alcohol is considered a drug.

- National prosperity requires a Healthy Workforce.
    - more than technology, industrial capability, or natural resources.
- Most drug users are employed (74.9%).
- Affects productivity, turnover, accidents, insurance costs, theft, higher use of benefits, profits, liability, negative public exposure.
- Makes organizations less competitive and less successful.

Historical Perspective

- Opium may be the oldest drug used by man.
    - Orally, smoked, pulverized, suppository form.
    - 1500 Egyptians.
    - 18th c. Europe.
    - 1800s – morphine and codeine.
    - Heroin (morphine derivative) – used for treatment of morphine addiction.
    - 19th c. – used mostly by middle and upper middle classes.

Legal Controls

- 1880 – US and China – agreement to prohibit shipment.
- 1930s – unlawful to possess or cultivate marijuana in the US.
- 1909 – federal act that limited the use of opium and derivatives for medical purposes.
- 1914 Harrison Act – only physicians could dispense narcotics.
- 1956 Narcotic Drug Control Act – mandatory minimum penalty of 5 years with no parole/probation for the first sale.
- Methadone – eventually used as a substitute for heroin.
    - Morphine ---- heroin ----methadone.

War on Drugs

- 1971 President Nixon.
- As prices rose, more criminals entered the market.
- 1988 President Reagan – Office of National Drug Control Policy (ONDCP)-
    - director is the “drug czar”.

Jonathan Taormina, CPP, CFE, PCI

Human Cost of Substance Abuse

- absent 16 times more often.
- Claim 3 times as many sickness benefits.
- File 5 times as many workers' compensation cases.
- Nonalcoholic family members of alcoholics use 10 times more sick.
- Children of alcoholics – 5 times more likely to become alcoholics.
- Less productive and creative.
- 20% who consume 80% of management's time.

Role of the Employer

- workplace problem.

- Rationalization – doesn't affect work performance.
- Opportunity:
- They know one another – contact is not suspicious.
- Better quality and fairer quantity – they know each other.
  - Workplace dealers want repeat customers.
- Low risk/High return on investment.
- Ability to buy and sell on credit:
  - "Fronted" drugs – paid for later.
  - "Pinch" – premium for fronted drugs – small amount kept for personal use by the seller.

Path of Workplace Substance Abuse

- usually begins with experimentation.
- Defend the drug's benefit, value to society, and their right to use it.
- Performance deteriorates and eventually they begin to use at work.
  - Enjoy testing the boundaries of acceptable behavior.
  - May keep drugs in desks, lockers, toolboxes, etc.
- Resourceful, cunning, and deceitful.
- Socialize more than others – networking.
- Avoid interaction with management.
- Resist team building – enjoy creating strife between management and labor.
- If they begin to steal, the principle victim will be the employer.
- Often begins with stealing food from coworkers.
- Steal from customers and vendors.
- Have accidents and get injured.
- False claims and fake on-the-job injuries – to escape discipline.
  - Extended absence – return more chemically dependent, less productive, and more likely to file a claim.

Jonathan Taormina, CPP, CFE, PCI

Drugs of Abuse

<u>Controlled Substance Act (CSA)</u>

Comprehensive Substance Abuse Prevention and Control Act of 1970, Title II.

- Mechanisms for reducing availability.
- Procedures for bringing a substance under control.
- Criteria for determining control requirements.
- Obligations incurred through international treaties.
- DEA – responsible for enforcement and oversees the classification.
    - Schedule I – high potential for abuse, **<u>no</u>** accepted medical use.
        - Hashish, marijuana, heroin, lysergic acid diethylamide (LSD).
    - Schedule II – high potential for abuse, has an accepted medical use.
        - Cocaine, morphine, amphetamine, phencyclidine (PCP).
    - Schedule III – less potential for abuse, has an accepted medical use.
        - Codeine, Tylenol with codeine, Vicodin.
    - Schedule IV – low potential for abuse, has accepted medical use.
        - Darvon, Darvocet, Phenobarbital, Valium.
    - Schedule V – low potential for abuse, has accepted medical use.
        - Low strength prescription cold and pain medicines.

<u>Depressants</u>

- Quaalude (methaqualone), Valium (diazepam), Librium (chlordiazepoxide), Nembutal (Phenobarbital), Seconal (secobarbital), **and Alcohol.**
- Calm feeling, impaired reflexes, slurred speech, drowsiness.
- <u>Alcohol:</u>
    - Fast acting, analgesic with sedative affects.
    - Addictive.
    - 4 symptoms: craving, loss of control, physical dependence, tolerance.
    - Need can be as strong as the need for food or water.

<u>Narcotics</u>

- Opiates, its derivatives, and synthetic substitutes.
- Pain relief.
- Highly addictive and frequently abused.
- Relatively uncommon in the workplace ????????????? (JT)
- Euphoric effect – "high" or "on the nod".
- Withdrawal – without intervention – disappears in 7-10 days.
    - Psychological dependence may continue.
- Some begin use for valid medical treatment.
- The younger the individual – more likely to progress to dependence/addiction.
- <u>Oxycodone:</u>
    - Schedule II.
    - 10 mg or oral Oxycodone = 10 mg. of subcutaneous Morphine.
    - Large dose can cause severe respiratory depression ---- death.

Stimulants

- may make employees appear more alert, eager, and productive.
- Actually leads to wasted efforts and mistakes.

Cocaine

- highly addictive.
- “wired” or “buzzed”.
- Deaths are often the result of cardiac arrest or seizures followed by respiratory arrest.
- “Binging” – taking the drug repeatedly and in increasing doses.
  - May lead to irritability, restlessness, and paranoia.

Methamphetamine

- synthetic drug.
- “Crank”, “meth”, “crystal meth”, or “speed”.
- Intense rush or “flash”.
- “Binge and Crash” – as tolerance increases, users binge to maintain the effects.
- Ice – smokable form of methamphetamine – in a glass pipe (like crack).
- Can elevate body temperature to dangerous levels.
- Formication – sensation of insects creeping on the skin.
- will forego food and sleep to go on a “run” (a form of binge).
- “wired”.
- Users are called “cranksters”.

Hallucinogens

- mind altering drugs. Most common:
  - LSD - Lysergic Acid Diethylamide – called “acid”.
  - MDA – Methylenedioxyamphetamine.
  - MDMA – Methyllenedioxymethamphetamine – called “ecstasy”.
  - PCP – phencyclidine – called “angel dust”.
  - Mescaline – from peyote cactus.
  - Certain mushrooms.
- Do not always produce hallucinations.
- Synaesthesia – sensory crossover – see sound or smell colors.
- Flashbacks – can happen months after use.

LSD – one of the most powerful hallucinogens.

- ingested orally it’s called “acid”, “blotter acid”, “window pane”, “microdots”, and “mellow yellow”.
    - “Tripping”.

PCP – originally compounded as an anesthetic for large animals.

- discontinued – too unpredictable.
- “angel dust” – typically applied to tobacco or marijuana cigarette.
  “Dusted”.

Marijuana

- 2nd most common drug of abuse after alcohol.
- Derived from hemp plant, cannabis sativa.
- Tetrahydrocannabinol (THC) – principle psychoactive component.
    - Retained in the fatty tissue and accumulates.
    - User become less tolerant and requires less of it (Reverse Tolerance).
        - "stoned" or "buzzed".

Hashish

- consists of THC-rich resinous material of the cannabis plant.

Analogue or Designer Drugs

- synthetic preparation.
- NOT initially classified as a controlled substance.

Prescription Drugs

- frequently abused in the workplace.
- Stimulants and sedatives.
- Most common sold at work – family of drugs called benzodiazepines:
    - Benzodiazepines – designed to relieve anxiety, tension, and muscle spasms.
        - Librium, Xanax, Valium.
    - Abuse particularly high among heroin and cocaine abusers.
- Flunitrazepam (Rohypnol) – not legally manufacture in the US.
    - "rophies", "roofies", "roach".
    - Party drug, rape drug.

Addiction and Chemical Dependency

Addiction – the disease of COMPULSION to anything.

- Stage One	Increased tolerance. Lying about how much and how often.
- Stage Two	Rationalization.
- Stage Three	Obsession. Frequently terminal.

- Addictions are treatable.

Chemical Dependency

- integral component of addiction.
- Physiological cravings brought on by chemical changes in the body.
    - Mental and physical changes.
- Tolerance – larger doses are required.
- Withdrawal – result of the body's attempt to chemically adapt in the absence of the drug.

Functional Abusers

- may require the drug just to function “normally”.
- When deprived, they are entirely different people.

Denial

- refuse to believe or consciously acknowledge their behavior is harmful.
- Rationalize
- Minimize
- Friends and coworkers may be in denial and may actually encourage the abuser to continue by suggesting the behavior is normal
- Supervisors/Managers/Organizations may be in denial.
    - Organizations in denial deny the abuser the help they need.

Enabling

- consciously or unconsciously allowing or encouraging the destructive behavior of others.
- Extends from denial.
- Feeds the abuser’s rationalizations.
- Family members enable when they forgive.
- Easier to enable than to confront reality.
    - Breaking the cycle requires honest confrontation.

Codependency

- allowing the behavior of another to overshadow their own values and judgment.
    - Not standing up for what one knows is right.
    - Fear of rocking the boat.
    - Become rescuers, caretakers, complainers, and adjusters.
    - May actually join the abuser.

- Supervisors/managers must be able to recognize the destructive behaviors of denial, enabling, and codependency.

Role of Supervisors and Managers

Drug-Free Workplace Policy

- absolutely necessary and equitably enforced.
- Acknowledged in writing by every employee.
- How/when drug testing will be performed and consequences for failing to provide a specimen.
- Recognize drug problems are treatable and explain treatment and rehabilitation options.
- EAP – Employee Assistance Programs.
- “Under the Influence” – only a legal term for alcohol. Proving that an individual is under the influence of anything other than alcohol is not possible.

- Institute an appropriate waiting period during which you educate employees.
- Monitor performance – not expected to catch employees.

Investigation and Documentation

- investigation is a fact-finding process, ideally separated from the decision-making process.
- Well documented and must protect the rights of violators and witnesses.
- Confidential – but management and HR always included.

Employee Hot Lines - open door policies are not enough.

Legal Mandates

- Sarbanes-Oxley (SOX) – requires proper “receipt, retention, and treatment of complaints”.
- Multinationals – required in some countries, illegal in others
- European countries – uneasy about employees who report anonymously.

Early Warning System

- anonymous employee hotlines allow for misconduct to be detected sooner than they might otherwise be without – Limit losses and protect reputation.
- Shows employees that concerns are taken seriously.

Selecting a System – outsourcing might have the advantage of better technology and better trained call takers.

Intervention – the calculated interruption of the destructive behaviors.

- not discipline, but rather a caring behavior to plan, prepare, and act.
- Attempt to salvage the troubled employee.
- Tool designed to correct, not punish.
- Can prevent unnecessary discipline, turnover, and may save a life.

- Employee performance must be documented.
- Observe an document performance.
- Confront the employee in private.
- Interview and discuss – only specifics, NEVER generalize.
  - provide employee proof of substandard performance.
  - offer employee the opportunity to provide an explanation.
  - ask how the organization can help the employee meet expectations.
  - Empathize but do not make a commitment.
  - Advise the employee of the company’s EAP.
  - Conclude on a positive note.
  - Send employee back to work.
- Document results.
- Communicate with upper management and HR.
- Follow up.

When Intervention Fails

- discipline may be the only answer.
- Documented progressive discipline is the incremental escalation of discipline in response to continued performance shortcomings.

Employee Assistance Programs

- 1940s – known as occupational alcoholism programs.
- Today – alcohol/substance abuse, family problems, marital, and other personal issues.
- Usually available to family members.
- Employee and family members are called “clients”.
- EAP professionals develop a community referral network – client must follow up.
- EAP monitors - treatment is provided by independent, outside professionals.
- Americans with Disabilities Act (ADA)
    - Includes recovering abusers NOT current users.
- If management referral – participation is mandatory.

Behavior Modification through Role Modeling

- positive peer pressure. Setting an example.

Reintegration of the Recovering Employee – healthy and caring culture.

Employee Education and Supervisor Training

- training for employees at all levels.

Drug Testing

- Drug Free Workplace Act of 1988 – businesses contracting with the federal government and receiving grants over $25,000.
- Other regulations require periodic testing in transportation and public service industries.

Methods

- biological specimen – urine, blood hair, saliva.
- Metabolite – chemical byproduct left behind after body metabolizes…
- Split sample – part for testing and a part preserved.
- Immunoassays, radioimmunoassay (RIA), and thin-layer chromatography (TLC).
    - TLC is most common and least expensive.
    - RIA is most accurate.
- If positive preliminary test – a confirmatory test is used.
    - High performance liquid chromatography, gas chromatography, and gas chromatography/mass spectrometry (GC/MS – most accurate).

Jonathan Taormina, CPP, CFE, PCI

Accuracy – extremely accurate.

- 1 out of 1 million result in false positive.
- Certification by the national Institute On Substance Abuse (NIDA).

Strategy

- may be limited by federal/state law, CBAs and contractual obligations.
- DHHS-5 (Department of Health and Human Services 5:
    - Alcohol + 5 – marijuana, cocaine, amphetamines, opiates and PCP.
- Consider the impact of the ADA which limits medical inquiries by employers.
    - BUT under the ADA, a drug test is NOT considered a medical examination….BUT AN ALCOHOL TEST IS.
- Advisable to test only after an employment offer is made

When should testing be performed?

- most difficult and controversial decision (before an offer is made, upon reasonable suspicion, after an accident/injury, random basis. After return to work following a violation, follow up to treatment?)
- Reasonable-suspicion testing – found to be more effective than random testing.

What type of testing? – urine, saliva, blood, hair, or breath?

Who should be tested?

- may not be employer's ultimate decision (ie. CBAs = bilateral decision).
- Only safety sensitive workers randomly.

Who should collect the specimens?

- federal regulations require collector to be "qualified".
- Alcohol tests – breath alcohol technicians.
- Alcohol screening – screen test technicians.

Where should the specimens be collected?

- job site or medical facility?
- Some CBAs require DHHS-certified or CAP-approved facility.

Who should receive the results?

- reviewed by a medical review officer (MRO).
- Treated as confidential medical information.

<u>Employer Incentives</u>

- reduced annual premiums or presumed denial of benefits under the worker's compensation laws.
- Need not pay if:
    - Worker violated a known safety rule, AND
    - Worker's intoxication is the cause of the injury.
- Case law:
    - Drunk contractor fell off roof = no payment.
    - Aide worker lifting patient = received payment.
- Immunity from prosecution/lawsuits if termination is the result of a positive drug test or refusal.

<u>Liability</u>

- poorly managed programs can lead to costly outcomes in court.
- Chain of custody – if broken, results are invalid
- Must design sound written policies and be prepared for ever-changing rules and regulations.

Can you test positive as a result of secondhand MJ smoke? NO
Do drug test violate rights? Are they discriminatory? NO

- employers have the right to drug-free workplace.

Window of detection – length of time drugs remain detectable.

US Federal Regulation

<u>Vocational Rehabilitation Act</u> – does not include someone currently using.

- an individual with a disability is one who completed treatment and is no longer using.

<u>Americans with Disabilities Act (ADA)</u> – the test to determine the use of **illegal drugs** shall NOT be regarded as a medical examination.

<u>Drug Free Workplace Act</u> – imposes duties on entities that contract with the federal government or receive grants to maintain a drug-free workplace.

<u>Family and Medical Leave Act (FMLA)</u>

- employers of 50 or more employees.
- Leave up to 12 weeks for employees employed for 12 months, who have worked 1250 hours in the previous 12 month period.
- Employee is reinstated to the same or equivalent position and suffers no loss of benefits or seniority (Does NOT apply to salaried employees in the top 10% of the workforce).

Illegal Drugs – not legally obtainable, or legally obtainable but has not been legally obtained, or drugs not being used for prescribed purposes.

Jonathan Taormina, CPP, CFE, PCI

CHAPTER 12 ADDRESSING WORKPLACE VIOLENCE THROUGH VIOLENCE RISK ASSESSMENT AND MANAGEMENT

Alienists – now called psychiatrists.

Psychiatrists/Psychologists who only use their judgment are only 40 to 70 percent accurate in predicting violence.

- clinical judgments alone rarely outperform actuarial approaches alone.
- Specialty called violence risk assessment and management.

Most workplace homicides result from robberies and similar criminal violence.

Conceptual Framework

- violence risk assessment provides information that aids in appropriate allocation of resources to minimize harm.
- Aim first to divert.
- If diversion is unsuccessful, to delay.
- Diversion, delay, and response are the last elements in the program.
- Most distinctive and important elements are:
    - Behavioral recognition, notification, assessment, and intervention by planned disruption.
- Coordinated response: legal, human resources, security, behavioral, and other organizational and community elements.

Focus Areas

- reasonable cause to believe that someone may commit an act of violence.
- Employer has an obligation to protect the potential victim
- Violence Risk Assessment Program:
    - Inappropriate workplace conduct, harassment, intimidation, discrimination should be seen as related to the violence risk assessment.
    - Early warning signs.
- Business Related Concerns:
    - Liability, productivity, workplace morale, and associated costs.
    - Liable for negligence in lawsuits claiming negligent security.
    - Greatest economic loss - loss of morale and productivity.

Liability and Legal Considerations

- various laws and regulations require US employers to provide a safe workplace.
- Company should research, document, and understand the method by which employees can obtain restraining or protective orders.
    - Studies have shown that the majority of protective or restraining orders aid in the cessation of violence.
    - However, it is important to obtain them early in the cycle of violence.

Behavioral Dynamic of Workplace Violence

(Corcoran)

- aggressors do not "snap" but go trough a process of emotional escalation or, in the case of psychopaths, non-emotional decision making.
- Asses their mental and emotional levels along a continuum of violent behavior and then develop a plan to divert them from violence through a case-specific use of communication, company resources, community resources, and the legal system.

Psychopathic vs. Affective (Emotion-based)

- intervention is much more complex when dealing with psychopaths.
- Only trained, experienced violence risk assessors should attempt to intervene in cases involving a potential psychopath.
- The vast majority of cases involve emotion-based aggressors (Affective).

Emotion-based aggressors

- In general, the continuum of violent behavior starts with general disgruntlement.
- Then as the situation escalates – actions escalate.
    - Intimidation, harassment, spoken/written threats, assaults, vandalism, battery, kidnapping, maiming, homicide/suicide.
        - Potential escalation curve (p. 365)
    - Ranking of aggressor behaviors by perceived emotional intensity.
- Particular attention should be paid to the aggressor's history of stressful events and reactions to them.
    - "the best predictor of future behavior is past behavior".

Incident Management Team (TMT) and Resources

- security management, human resources, legal (familiar with employment issues).
- Take reports, assess, gather information as necessary, intervene as appropriate.

Jonathan Taormina, CPP, CFE, PCI

Violence Risk Assessment Process

Notification

- policy, procedures, and training that direct reporting to those responsible for initial assessment for immediate risk.

Assessment

- if the aggressor's identity is not known – a valid violence risk assessment cannot be conducted.
- Valid violence risk assessments require a depth of information available only for known subjects.
- **This is the difference between Behavioral Investigative Analysis (Profiling)** and Violence Risk Assessment.
    - **Profiling** is used to exlude persons from a pool.
    - **Violence Risk Assessment** – focused on a particular individual's risk of committing a violent act.

Known subject assessment – three levels of assessment

- Initial – is there an immediate risk of harm?
- Threshold – if no immediate harm, a threshold assessment determines whether assessment should continue or only monitored.
- Comprehensive – if a predetermined threshold has been met.

Initial Assessment

- whether the situation calls for an immediate emergency response.
- Whether to evacuate the facility or in the case of a bomb threat, the employees best suited to search the premises.
- Firearm on premises = 360 degree evacuation to cover.
- Shooter outside – may require a lockdown. (Columbine showed this to be ineffective as kids were shot while huddled in the library)
    - "those that run live and those that hide die".
- Post incident assessment to help the company return to full operation.
    - What was known? When? What was done about it?

Threshold Assessment

- if the initial assessment suggests there is no significant possibility of immediate harm, then a threshold assessment is conducted to determine whether, based on the violence risk assessment thresholds determined by the company, the situation warrants further action or only monitoring.
- If a predetermined threshold is reached – a comprehensive assessment is triggered.

Jonathan Taormina, CPP, CFE, PCI

Comprehensive Assessment

- most detailed information and resources available to thoroughly assess the potential violence risk.
- Determine the aggressor's behavioral history and current stressors.
- Contacts with law enforcement, court records, financial, medical, relationships, substance abuse, weapons, employment history.
- Chronological order makes it possible to analyze patterns:
    - Cause and effect perspective.
- Spousal Assault Risk Assessment Guide (SARA), Coworkers – Risk Assessment Guideline Elements for Violence (RAGE – V).
- Violence Risk assessment is completed by assigning a value to the risk:
    - Low, moderate, or high.

Intervention and Nonemergency Situational Resolution

- safety of the identified target or targets.
- Divert or deflect the aggressor.
- An unwilling resolution is likely only temporary:
    - Restraining/protective orders are "short term".
- Any form of communication or interaction, whether direct or indirect (through other parties), should be considered an intervention.

Monitoring

- monitoring creates the behavioral feedback loop.
- Passive monitoring – relies on the target and others who might witness new behavior to report to the IMT.
    - Effective only in low-risk cases.
    - "wait and see approach".
- Active monitoring – the assessor actively pursues new behavioral information.
    - The more elevated, the more contacts made.
    - Best option for moderate to high risk or if the target cannot be relied on to report new behavior.
        - Target may conceal or play down any contact from the aggressor.

Review and Debriefing – allows for continuous improvement.

- Incident review – ongoing basis.
- Debriefing – lessons learned for incident management and process improvement.
    - Strategy level look.

Future of Workplace Violence

- Functional magnetic resonance imaging (fMRI) is currently being explored for use in mapping brain function to detect deception in individuals.
- Nothing is more important than safety and security of personnel.