Ethics in Information Technology, Fourth Edition

Chapter 3
Computer and Internet Crime

George W. Reynolds

Lecturer : Mansour Rousta Zadeh

اصول اخلاقی در فناوری اطلاعات – ویرایش چهارم (جورج دبلیو رینالدز)

- درس اخلاق حرفه‌ای در فناوری اطلاعات
  - مدرس : منصور روستازاده
- فصل سوم ، گفتار دوم
  - جرایم کامپیوتری و اینترنتی
- هفته هفتم
  - نیمسال دوم ۹۲-۹۳

SMS : 0939 – 101 0024
eMail : EIT @ EXIST . IR

Types of Perpetrators

- Perpetrators include:
  - Thrill seekers wanting a challenge
  - Common criminals looking for financial gain
  - Industrial spies trying to gain an advantage
  - Terrorists seeking to cause destruction
- Different objectives and access to varying resources
- Willing to take different levels of risk to accomplish an objective

انواع مرتکبین جرم

- مرتکبین جرم شامل موارد زیر هستند:
  - افراد ماجراجوئی هستند که می خواهند مبارزه طلبی کنند
  - مجرمین معمولی که به دنبال منفعت های مالی هستند.
  - جاسوسان صنعتی که سعی در بدست آوردن مزایای رقابتی هستند.
  - تروریست هائی که به دلایل خاص خود در پی تخریب هستند
- (هر مرتکب جرم) اهداف متفاوت داشته و دسترسی به منابع مختلفی دارند
- (هر کدام) تمایل به پذیرش سطوح مختلفی از خطر دارند تا به هدف خود دست یابند

Types of Perpetrators (cont'd.)

TABLE 3-4 Classifying perpetrators of computer crime

Type of perpetrator	Typical motives
Hacker	Test limits of system and/or gain publicity
Cracker	Cause problems, steal data, and corrupt systems
Malicious insider	Gain financially and/or disrupt company's information systems and business operations
Industrial spy	Capture trade secrets and gain competitive advantage
Cybercriminal	Gain financially
Hacktivist	Promote political ideology
Cyberterrorist	Destroy infrastructure components of financial institutions, utilities, and emergency response units

Source Line: Course Technology/Cengage Learning.

انواع مرتکبین جرم

- دسته بندی مرتکبین جرائم کامپیوتری

نوع مرتکبین	انگیزه های معمول
هکر	محدوده های سیستم را تست می کند و/یا معروفیت پیدا می کند.
کرکر	ایجاد مشکل می کند داده ها راسرقت کرده و سیستمها را معیوب می کند.
نفوذی بدخواه	منفعت مالی کسب می کند و/یا سیستم های اطلاعاتی و عملیات کسب و کار شرکت را مختل می کند.
جاسوسی صنعتی	رازهای تجاری را کشف کرده و مزایای رقابتی را کسب می کند.
مجرمین سایبری	منفعت مالی کسب می کند.
هکر فعال سیاسی یا اجتماعی	ایدئولوژی سیاسی را ترویج می دهد
تروریست اینترنتی	مولفه های زیربنائی موسسات مالی ، تجهیزات و واحدهای پاسخگوی اضطراری را تخریب می کند

Hackers and Crackers

- Hackers
  - Test limitations of systems out of intellectual curiosity
    - Some smart and talented
    - Others inept; termed “lamers” or “script kiddies”
- Crackers
  - Cracking is a form of hacking
  - Clearly criminal activity

هکرها و کرکرها

× هکرها

- محدودیتهای سیستم های اطلاعاتی را محض کنجکاوی ذهنی شان تست می کنند(تا ببینند که آیا می توانند دسترسی پیدا کنند و اینکه چقدر میتوانند جلو بروند)
  - بعضی هکرها زیرک و با استعداد هستند.
  - بسیاری از آنها از نظر فنی بی عرضه هستند. هکرهای ماهرتر آنها را احمق ها یا بچه برنامه‌نویس می خوانند.
  - بعضی ها معتقدند که هکرها با شناسائی نقاط ضعف امنیتی در واقع خدمات رسانی می کنند.
  - ولی به مفهوم منفی امروزی بیشتر نزدیک است تا به مفهوم مثبتی که سابق داشته است.

× کرکر

- فرمی از هکینگ است
- به وضوح یک فعالیت مجرمانه است

× کرکرها بدون اجازه وارد سیستم ها و شبکه های دیگر می شوند تا به آنها صدمه بزنند

Malicious Insiders

- Major security concern for companies
- Fraud within an organization is usually due to weaknesses in internal control procedures
- Collusion
  - Cooperation between an employee and an outsider
- Insiders are not necessarily employees
  - Can also be consultants and contractors
- Extremely difficult to detect or stop
  - Authorized to access the very systems they abuse
- Negligent insiders have potential to cause damage

نفوذی های بدخواه

- **یکی از نگرانی های امنیتی مهم برای شرکت ها**
- **کلاهبرداری که در یک سازمان اتفاق می افتد معمولا به سبب ضعف در رویه های کنترل داخلی آن شرکت است.**
- **تبانی**
  - **همکاری بین یک کارمند و یک فرد خارجی است**
- **نفوذی ها لزوما کارمند نیستند**
  - **بلکه می توانند مشاورین و پیمانکاران باشند**
- **کشف یا متوقف ساختن نفوذی های بدخواه به شدت دشوار است**
  - **زیرا آنها اغلب اجازه ی دسترسی به بسیاری از سیستم هائی را دارند که از آن سوء استفاده می کنند.**
- **کارمندان داخلی مسامحه کار پتاسیل آن را دارند که باعث خطر شوند.**

Industrial Spies

- Use illegal means to obtain trade secrets from competitors
- Trade secrets are protected by the Economic Espionage Act of 1996
- Competitive intelligence
  - Uses legal techniques
  - Gathers information available to the public
- Industrial espionage
  - Uses illegal means
  - Obtains information not available to the public

جاسوسان صنعتی

- از ابزارهای غیر قانونی برای دستیابی به رازهای تجاری رقبای مالی خود استفاده می کنند.
- رازهای تجاری تحت حمایت قانون جاسوسی اقتصادی سال ۹۶ قراردارند.
  - که استفاده از یک راز تجاری برای استفاده شخصی یا منفعت خود و دیگری را به یک جرم تعبیر می کند.
  - رازهای تجاری غالبا توسط نفوذی هایی همچون کارمندان ناراضی و کارمندان سابق سرقت می شوند.
- هوش رقابتی
  - از تکنیکهای قانونی استفاده می کند.
  - و به منظور جمع آوری اطلاعاتی که در دسترس عموم قرار دارند می باشد
  - مثلا شرکت کنندگان ، اطلاعات بدست آمده از گزارش های مالی، ژورنال های تجاری، بایگانی عمومی و مصاحبه های چاپ شده با مسئولین شرکت را گردآوری و تحلیل می کنند.
- جاسوسی صنعتی
  - استفاده از ابزارهای غیر قانونی است.
  - به منظور دستیابی به اطلاعاتی است که در دسترس عموم قرار ندارد.
  - می تواند شامل سرقت طرح های محصولات جدید، داده‌های تولید، اطلاعات بازاریابی یا سورس کدهای نرم افزار

Cybercriminals

- Hack into corporate computers to steal
- Engage in all forms of computer fraud
- Chargebacks are disputed transactions
- Loss of customer trust has more impact than fraud
- To reduce potential for online credit card fraud:
  - Use encryption technology
  - Verify the address submitted online against the issuing bank
  - Request a card verification value (CVV)
  - Use transaction-risk scoring software

مجرمین سایبری

- **هک کردن کامپیوترهای صنفی با هدف سرقت**
  - **اغلب با انتقال پول از یک حساب به حساب (های) دیگر صورت می گیرد تا رد بسیار پیچیده و نامعلومی را برای پیگردی مامورین قانون از خود باقی بگذارند.**
  - **در تمامی شکل های کلاهبرداری کامپیوتری شرکت می کنند. به دلیل آنکه پتانسیل کسب منفعت های مالی زیاد است، خرج بسیاری بابت خرید تخصص فنی و سطح دسترسی از طریق نفوذی های بدخواه می کنند.**
  - **چارج بک ها تراکنش های معوقی هستند که ممکن است بر سر آن اختلاف وجود داشته باشد.**
    - **از دست رفتن اعتماد مشتریان تاثیر به مراتب بیشتری نسبت به هزینه خریدهای کلاهبردارانه و پشتیبانی امنیتی آنها دارد (می تواند تا حد زیادی حاشیه سود یک فروشنده اینترنتی را کاهش دهد.)**
  - **برای کاهش پتانسیل کلاهبرداری کارت اعتباری اینترنت آنلاین**
    - **استفاده از فناوری رمز گذاری با هدف حفاظت از اطلاعات بدست آمده از مصرف کنندگان**
    - **بررسی آنکه آیا آدرس ارائه شده به صورت آنلاین با آدرسی که بانک در دسترس دارد مطابقت دارد.**
    - **درخواست تایید کارت یا CVV برای جلوگیری از خرید با کارت های اعتباری که بطور آنلاین سرقت شده.**
    - **استفاده از نرم افزار امتیازدهی خطر-تراکنش که الگوهای تاریخچه خرید مشتری را دنبال می کند.**

Cybercriminals (cont'd.)

- Smart cards
  - Contain a memory chip
  - Updated with encrypted data each time card is used
  - Used widely in Europe
  - Not widely used in the U.S.

مجرمین سایبری

- **کارت های هوشمند**
  - **حاوی یک چیپ حافظه است**
  - **با هر با استفاده شدن کارت، با داده های رمزگذاری شده به روز می شود**
    - **داده رمزگذاری شده ممکن است شامل شناسائی حساب کاربر، میزان اعتبار باقی مانده باشد**
  - **کارت های هوشمند بطور وسیعی در اروپا استفاده می شود**
  - **ولی در ایالات متحده معروفیت را ندارند و بطور وسیعی استفاده نمی شود**
    - **و سبب هزینه های تبدیل پول برای فروشندگان می باشد**

Hacktivists and Cyberterrorists

- Hacktivism
  - Hacking to achieve a political or social goal
- Cyberterrorist
  - Attacks computers or networks in an attempt to intimidate or coerce a government in order to advance certain political or social objectives
  - Seeks to cause harm rather than gather information
  - Uses techniques that destroy or disrupt services

هکرهای فعال سیاسی یا اجتماعی و تروریست های سایبری

- **هکرهای فعال سیاسی یا اجتماعی(ترکیبی از کلمات Hack و Activism)**
  - **نوعی هک کردن به منظور دستیابی به اهداف سیاسی یا اجتماعی**
- **تروریست سایبری**
  - **حملات کامپیوتری را علیه کامپیوترها یا شبکه های دیگر اجرا می کند و این در تلاشی برای ترساندن یا وادار کردن یک دولت با هدف پیشبرد مقاصد سیاسی یا اجتماعی خاص صورت می گیرد**
  - **تروریست ها در نیل به اهداف شان افراطی تر از هکرهای فعالی سیاسی اجتماعی هستند.**
  - **به دنبال صدمه زدن هستند تا جمع آوری اطلاعات**
  - **از تکنیک هائی استفاده می کنند که سرویس های مختلف را تخریب یا مختل کنند.**

Federal Laws for Prosecuting Computer Attacks

TABLE 3-5 Federal laws that address computer crime

Federal law	Subject area
USA Patriot Act	Defines cyberterrorism and penalties
Identity Theft and Assumption Deterrence Act (U.S. Code Title 18, Section 1028)	Makes identity theft a Federal crime with penalties up to 15 years imprisonment and a maximum fine of $250,000
Fraud and Related Activity in Connection with Access Devices Statute (U.S. Code Title 18, Section 1029)	False claims regarding unauthorized use of credit cards
Computer Fraud and Abuse Act (U.S. Code Title 18, Section 1030)	Fraud and related activities in association with computers: • Accessing a computer without authorization or exceeding authorized access • Transmitting a program, code, or command that causes harm to a computer • Trafficking of computer passwords • Threatening to cause damage to a protected computer
Stored Wire and Electronic Communications and Transactional Records Access Statutes (U.S. Code Title 18, Chapter 121)	Unlawful access to stored communications to obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage

Source Line: Course Technology/Cengage Learning.

Implementing Trustworthy Computing

- Trustworthy computing
  - Delivers secure, private, and reliable computing
  - Based on sound business practices

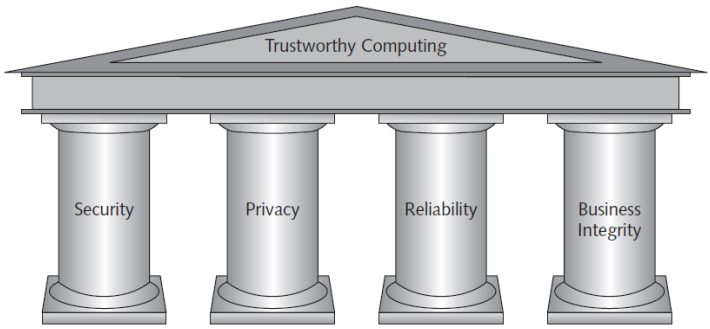

FIGURE 3-4 Microsoft's four pillars of trustworthy computing
Source Line: Course Technology/Cengage Learning.

پیاده سازی محاسبات امن

- **محاسبات امن**
  - **روشی است که محاسبات قابل اطمینان، خصوصی و ایمن را**
  - **بر اساس تجربیات کسب و کار سالم ارائه می دهد.**
  - **به عنوان مثال مایکروسافت تعهد کرده است که ابتکار عملیات محاسبات امنی را ارائه کند که با هدف ارتقای سطح اعتماد به محصولات نرم افزاری اش طراحی شده است که چهار ستون آن عبار تست از**
    - **امنیت**
    - **حریم**
    - **قابلیت اطمینان**
    - **درستی(تمامیت) کسب و کار**

Implementing Trustworthy Computing (cont'd.)

- Security of any system or network
  - Combination of technology, policy, and people
  - Requires a wide range of activities to be effective
- Systems must be monitored to detect possible intrusion
- Clear reaction plan addresses:
  - Notification, evidence protection, activity log maintenance, containment, eradication, and recovery

پیاده سازی محاسبات امن

- **امنیت هر سیستم یا شبکه**
  - **ترکیبی از فناوری ، سیاست و افراد**
  - **به دامنه ی وسیعی از فعالیت ها که تاثیرگذار باشند نیازمند است.**
- **سیستمها باید تحت نظارت و کنترل قرار بگیرند که هرگونه نفوذ احتمالی را کشف کند.**
  - **چراکه هیچ سیستم امنیتی کامل نیست .**
- **باید طرح واکنش روشنی وجود داشته باشد که بتواند موارد زیر را انجام دهد:**
  - **هشدار دادن**
  - **حفاظت از شواهد**
  - **حفاظت از لیست ثبت فعالیت ها**
  - **محدود کردن**
  - **ریشه کن سازی**
  - **بازیابی**

Risk Assessment

- Process of assessing security-related risks:
  - To an organization's computers and networks
  - From both internal and external threats
- Identifies investments that best protect from most likely and serious threats
- Focuses security efforts on areas of highest payoff

ارزیاب ریسک

- فرآیند ارزیابی خطرات امنیتی :
  - متوجه کامپیوترها و شبکه های یک سازمان
  - از تهدیدات داخلی و خارجی است
- شناسائی آن سرمایه گذاری های زمان و منابع است که می تواند به بهترین شکل از سازمان در برابر محتمل ترین و جدی ترین تهدیدات حفاظت کند.
- بر میزان امنیت روی نواحی که بیشترین بازدهی را دارد متمرکز است.
- دارائی : به هر سخت افزار، نرم افزار، سیستم کامپیوتری، شبکه یا پایگاه داده اطلاق می شود که سازمان با هدف نیل به اهداف کسبو کار خود از آن استفاده می کند
- رویداد خسارت : هر نوع رخدادی است که تاثیر منفی بر یک دارائی دارد

Risk Assessment (cont'd.)

- Eight-step risk assessment process
  - #1 Identify assets of most concern
  - #2 Identify loss events that could occur
  - #3 Assess likelihood of each potential threat
  - #4 Determine the impact of each threat
  - #5 Determine how each threat could be mitigated
  - #6 Assess feasibility of mitigation options
  - #7 Perform cost-benefit analysis
  - #8 Decide which countermeasures to implement

ارزیابی ریسک – ادامه

- **هشت گام فرآیند ارزیابی ریسک**
  - **شناسائی دارائی هائی که سازمان بیشترین نگرانی را در رابطه با آن دارد.**
  - **شناسائی رویدادهای خسارت ، خطرات یا تهدیداتی که ممکن است رخ دهد.**
  - **ارزیابی دفعات یا احتمال وقوع رویدادها یا تهدیدات**
  - **تعیین تاثیر هر تهدیدی که رخ دهد.**
  - **تعیین اینکه چگونه می‌توان هرتهدید را به گونه‌ای تخفیف داد که احتمال وتاثیر وقوع به مراتب کمتری پیدا کند.**
  - **ارزیابی امکان پذیری استفاده از گزینه های تخفیف احتمال و تاثیر وقوع تهدیدات**
  - **انجام تحلیل هزینه/مزایا به منظور حصول اطمینان از اینکه آیا تلاش ها مقرون به صرفه است**
  - **تصمیم گیری براینکه کدام اقدام متقابل خاص باید استفاده شود.**
- **تضمین معقول**(Reasonable Assurance)
  - **حاکی ازآن است که مدیران می بایست ازقضاوت خود استفاده کنند تا مطمئن شوند که هزینه کنترل از مزایای سیستم یا خطرات درگیر فراتر نخواهد رفت.**

Risk Assessment (cont'd.)

TABLE 3-7 Risk assessment for hypothetical company

Risk	Business objective threatened	Estimated probability of such an event occurring	Estimated cost of a successful attack	Probability × cost = expected cost	Assessment of current level of protection	Relative priority to be fixed
Distributed denial-of-service attack	24/7 operation of a retail Web site	40%	$500,000	$200,000	Poor	1

(*Continued*)

Risk Assessment (cont'd.)

Risk	Business objective threatened	Estimated probability of such an event occurring	Estimated cost of a successful attack	Probability × cost = expected cost	Assessment of current level of protection	Relative priority to be fixed
Email attachment with harmful worm	Rapid and reliable communications among employees and suppliers	70%	$200,000	$140,000	Poor	2
Harmful virus	Employees' use of personal productivity software	90%	$50,000	$45,000	Good	3
Invoice and payment fraud	Reliable cash flow	10%	$200,000	$20,000	Excellent	4

Source Line: Course Technology/Cengage Learning.