Developing an E-commerce Security Plan

1. Perform a risk assessment
2. Develop a security policy
3. Develop an implementation plan
4. Create a security organization
5. Perform a security audit

Figure 4.12, Page 287
A Security Plan: Management Policies

**Risk assessment**

- What information assets are at risk?
  - Customer information
  - Patented designs
  - Secret processes
  - Financial information: Price schedules, employee compensation, payroll

- Basic steps:
  1. For each type of information asset, estimate the value (in Euros) if it were compromised
  2. Multiply that amount by probability of the loss
  3. Finally, rank order the results
Bow-Tie Analysis

## Example in the Chemical Industry

Risk factors, impacts, and mitigation strategies for the identified risks.

<table>
<thead>
<tr>
<th>Identified risk</th>
<th>Risk factors</th>
<th>Risk impacts</th>
<th>Preventive barriers</th>
<th>Protective barriers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-conforming product (R1)</td>
<td>○ Release of wrong raw materials (F11)</td>
<td>○ Customer dissatisfaction (L11)</td>
<td>○ Materials are issued via computerized system (V11)</td>
<td>○ Materials are revised by line Q.C. before releasing them from warehouse (C11)</td>
</tr>
<tr>
<td></td>
<td>○ Addition of the wrong chemical into a certain batch by mistake (F12)</td>
<td>○ Loss of reputation (L12)</td>
<td>○ Materials are released with an identification sticker on pallet by line Q.C. supervisor (V12)</td>
<td>○ Continuous supervision by the Q.C. supervisor during production (C12)</td>
</tr>
<tr>
<td></td>
<td>○ Insufficient cleaning of tanks &amp; pipes (F13)</td>
<td>○ Waste of money (L13)</td>
<td>○ Perform a checklist for the line prior to production and adding cleaning as the last step in a batch filling (V13)</td>
<td>○ Q.C. inspection during filling (C13)</td>
</tr>
<tr>
<td>Personal injuries (R2)</td>
<td>○ Safety procedures are not followed by an employee (F21)</td>
<td>○ Absence of work (L21)</td>
<td>○ Application of warnings and penalties to those who doesn't follow the safety procedures and incentives to those who follow them (V21)</td>
<td>○ Periodic inspection by safety supervisor and installing cameras to continuously monitor any unsafe acts (C21)</td>
</tr>
<tr>
<td></td>
<td>○ Lack of awareness and supervision (F22)</td>
<td>○ Compensation (L22)</td>
<td>○ Increase awareness through periodic training courses (V22)</td>
<td>○ Installing safety signs to continuously bring attention to safety procedures (C22)</td>
</tr>
</tbody>
</table>
A Security Plan: Management Policies

Security policy

- Prioritizing the information risks
- Who generates and controls the information assets found in the risk assessment?
- What existing security policies are in place to protect the information?
- What enhancements can be recommended to improve security of the most valuable assets?
- What level of risk are you willing to accept?
  - Lose credit card data once every 10 years
  - 100-year hurricane strategy
A Security Plan: Management Policies

- Implementation plan
  - Security organization
    - Educates and trains employees
    - Keep management aware of security threats and breakdowns
    - Maintain tools chosen to implement security
  
- Access controls
  - Outsiders: Firewalls
  - Insiders: Login procedures (usernames and passwords), proxies

- Authentication procedures, including biometrics

- Authorization policies: Differing levels of access to information assets for differing user levels
A Security Plan: Management Policies (cont.)

- **Implementation plan**
  - Authorization management systems
    - Follows user from page to page in an encrypted user session
    - Access is allowed only to those areas that the user is permitted to enter
    - Each user type has specific entry rules

- **Security audit**
  - Review of access logs
  - Insight in how outsiders are using the site and how insiders are accessing the site’s assets
Govt. Policies and Controls on Encryption Software

- Regulation of the uses of encryption and restricting availability and export of encryption systems
  - Organization for Economic Cooperation and Development (OECD)
  - G-7 (heads of state of the top seven industrialized countries, excluding Russia)
  - European Council
  - Wassenaar Arrangement (41 countries that produce sensitive industrial equipment or weapons – ‘dual-use goods’)

- Both NSA and GCHQ (U.K.) may be able to break encryption schemes used by SSL/TLS, VPNs, and on 4G smartphones
### What are main reasons for why key escrow systems are largely abandoned?

<table>
<thead>
<tr>
<th>Regulatory Effort</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricted export of strong security systems</td>
<td>Supported primarily by the United States. Widespread distribution of encryption schemes weakens this policy. The policy is changing to permit exports except to pariah countries.</td>
</tr>
<tr>
<td>Key escrow/key recovery schemes</td>
<td>France, the United Kingdom, and the United States supported this effort in the late 1990s but now have largely abandoned it. There are few trusted third parties.</td>
</tr>
<tr>
<td>Lawful access and forced disclosure</td>
<td>Growing support in U.S. legislation and in OECD countries.</td>
</tr>
<tr>
<td>Official hacking</td>
<td>All countries are rapidly expanding budgets and training for law enforcement “technical centers” aimed at monitoring and cracking computer-based encryption activities of suspected criminals.</td>
</tr>
</tbody>
</table>
Basic requirements for key escrow

- Availability of highly sensitive and highly available secret key over an extended time period
- Quick access to decrypted information by law enforcement agencies without notice to the key owners
- What if you pre-encrypt information that is sent through a channel encrypted with the secret key that is in escrow?
## Govt. Policies and Controls on Encryption Software (cont.)

<table>
<thead>
<tr>
<th>REGULATORY EFFORT</th>
<th>IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricted export of strong security systems</td>
<td>Supported primarily by the United States. Widespread distribution of encryption schemes weakens this policy. The policy is changing to permit exports except to pariah countries.</td>
</tr>
<tr>
<td>Key escrow/key recovery schemes</td>
<td>France, the United Kingdom, and the United States supported this effort in the late 1990s but now have largely abandoned it. There are few trusted third parties.</td>
</tr>
<tr>
<td>Lawful access and forced disclosure</td>
<td>Growing support in U.S. legislation and in OECD countries.</td>
</tr>
<tr>
<td>Official hacking</td>
<td>All countries are rapidly expanding budgets and training for law enforcement “technical centers” aimed at monitoring and cracking computer-based encryption activities of suspected criminals.</td>
</tr>
</tbody>
</table>

Copyright © 2015 Pearson Education, Inc.
Forced Disclosure: 2015 San Bernardino Attack

- Stakeholders:

Source: https://en.wikipedia.org/wiki/2015_San_Bernardino_attack
Forced Disclosure:
2015 San Bernardino Attack

- On February 9, 2016, the FBI announced that it was unable to unlock one of the mobile phones they recovered, a county-owned iPhone 5C
- FBI asked Apple to disable certain security features but Apple declined
- FBI responds by issuing a court order, mandating Apple to disable the features

Source: https://en.wikipedia.org/wiki/2015_San_Bernardino_attack
Apple still denies, citing the security risks that the creation of a *backdoor* would pose towards their customers.

U.S. Department of Justice urges a federal judge to compel Apple to comply with the order.
The new application stated that Apple could install the malware on the phone on its own premises, and after the FBI had hacked the phone via remote connection, Apple could remove and destroy the malware.
Apple discusses four methods to access data in the iPhone with the FBI, but one promising method to backup data to iCloud was ruled out by a mistake.

FBI had already asked San Bernardino County, the owner of the phone, to reset the password to the perpetrator’s iCloud account to acquire data from the iCloud backup.
2015 San Bernardino Attack (cont.)

- However, this rendered the phone unable to back up recent phone data to iCloud unless its *passcode* is entered.
- The Department of Justice announced that it had unlocked the iPhone and withdrew its suit.
- Anonymous sources state that the Israeli company *Cellebrite* was assisting the FBI with this.
The Washington Post reported that the FBI instead paid hackers who used a zero-day vulnerability in the iPhone’s software to bypass its ten-try limitation, and did not need Cellebrite’s assistance.

$10^4 = 10000$ possibilities
E-commerce Payment Systems

- In U.S., credit and debit cards are primary online payment methods
  - In the Netherlands: iDEAL

- Cardholder Not Present (CNP) transactions
  - Merchant never sees the credit card
  - No hand-signed agreement to pay
  - Transaction may be disallowed and reversed when disputes arise
How an Online Credit Transaction Works

1. Consumer makes purchase
2. SSL/TLS provides secure connection through Internet to merchant server
3. Merchant software contacts clearinghouse
4. Clearinghouse verifies account and balance with issuing bank
5. Issuing bank credits merchant account
6. Monthly statement issued with debit for purchase

Figure 4.14, Page 295
How an Online Credit Transaction Works

1. Consumer makes an online purchase.
2. SSL/TLS provides secure connection through Internet to merchant server.
3. Merchant software contacts clearinghouse.
4. Clearinghouse verifies account and balance with issuing bank.
5. Issuing bank credits merchant account.

Does SSL authenticate the merchant or consumer?

Figure 4.14, Page 295
E-commerce Payment Systems (cont.)

- Payment Card Industry - Data Security Standard (PCI-DSS) compliance
  - Instituted by the five major credit card companies
  - Industry-mandated standard
E-commerce Payment Systems (cont.)

- Payment Card Industry - Data Security Standard (PCI-DSS) compliance
  - Six major control objectives:
    - Build and maintain a secure network
    - Protect cardholder data
    - Maintain a vulnerability management program
    - Implement strong access control measures
    - Regularly test and monitor networks
    - Maintain an information security policy
E-commerce Payment Systems (cont.)

Limitations

- Poor security
  - Neither merchant nor consumer can be fully authenticated

- Repudiation of charges: High risk for merchants

- Transaction costs
  - Roughly 3.5% of the purchase + transaction fee of ca. 30 eurocent per transaction

- Although ubiquitous, not very democratic
  - Millions of adults do not have credit cards
  - Millions of others who cannot afford them
Alternative Online Payment Systems

- Online stored value systems:
  - Based on value stored in a consumer’s bank, checking, or credit card account
  - Example: PayPal
  - No personal credit information has to be shared among the users
  - Relatively high cost
    - 2.9% - 5.99% of the amount plus a small fixed fee (typically 0.25 eurocent)
Mobile Payment Systems

- Use of mobile phones as payment devices
  - Established in Europe and Asia
    - Rabo Wallet, ING Mobiel Betalen
  - Expanding in United States
    - Apple Pay, Android Pay, Samsung Pay, PayPal, Square

- Near field communication (NFC)
  - Short-range (2”) wireless shares data between devices
  - New debit cards are equipped with NFC chips
Mobile Payment Systems: Apple Pay

- Customer should have credit card on file with iTunes
- Payment: Touch ID to ensure the phone belongs to the customer
- Customer swipes the phone near a merchant’s NFC point-of-sale terminal
- Digital token: Unique device number and generation of 1-time 16-digit code
Mobile Payment Systems: Apple Pay (cont.)

- **Transaction approval / denial (1 sec):**
  - Token is encrypted and sent to Apple servers for verification of authenticity of the phone and the customer
  - Credit card issuers verify account owner and available credit
  - Credit card information not shared with merchant nor transmitted from iPhone
  - 800 million stored credit cards are encrypted

**What is the key security advantage with this system?**
Mobile Payment Systems: Apple Pay (cont.)

- Credit card companies charge merchants a transaction fee
- Apple Pay will not charge the merchant nor consumer a fee
- Apple charges the credit card issuer bank a .15% fee in return for guaranteeing transaction authenticity
- ‘Insurance policy for credit card issuers’
Digital Cash and Virtual Currencies

- **Digital cash**
  - Based on algorithm that generates unique tokens that can be used in “real” world
  - Bitcoins are anonymous and are exchanged via a 34-character alphanumeric address

- **Virtual currencies**
  - Circulate within internal virtual world
  - Example: Linden Dollars in Second Life, Facebook Credits