How do we prevent, detect, respond and recover from CRM breaches?

Oct 27, 2010

Management Track: Session 7 10:20-11:20

Kelly Walsh CISSP CISM CPP

Q: What is a CRM breach?

A: Any event which results in the loss of availability or integrity of the RELATIONSHIP between you and your customers or clients

Good example of CRM breach - http://www.youtube.com/watch?v=IYDup1bguC4

Compare CRM Breach to Security Breach Impacts

CRM Breach

Results In:

- Loss of public image
- Loss of consumer confidence
- Direct loss of customer base
- Indirect loss of revenue

Security Breach

May Result In:

- Loss of Public Image
- Loss of consumer confidence
- Direct Loss of Assets or Revenue
- Indirect Loss of Customer Base

Q: So who or what causes CRM breaches?

Human Threat Agents (HTAs)

CRM Breaches

- HTAs
  - Usually not motivated
  - Almost always an internal resource
  - Few consequences if caught.
  - Most severe punishment loss of employment

Security Breaches

- HTAs
  - Normally motivated (profit, power, political/religious views, revenge, etc)
  - Can be either “insider” or external agents
  - Often severe legal consequences including imprisonment

Non-Human Threat Agents

CRM Breaches

- Failure of communication channel
  - Phone, Email, Fax
- Failure of service or product delivery channel
  - Shipping/Logistics
- Failure of product quality
  - Product breaks or fails before expected

Security Breaches

- Natural disasters
  - including fire
  - Flood
  - pandemic
- Environmental Failures
  - Power loss
  - Failed AC/Cooling
  - Broken water main
- Malfunctions of systems

Q: So how do we protect ourselves from CRM Breaches?

- A: The same way we protect ourselves from Security Breaches.

Risk Management

- ISO/IEC 27001:2005 Information Security Management System (ISMS) & ISO/IEC 27005:2008 Information Security Risk Management
  - Define risk assessment approach
  - Identify the risks
  - Analyze & evaluate the risks
  - Identify & evaluate options to manage the risk
  - Select control objectives & controls to manage risk

Introducing New Terms

- Customer Lifetime Value (CLV)
  - An estimated value (usually represented in $$$) calculated as the sum of a customer's past & current consumption of products and services, with their estimated lifetime future consumption
- Customer Relationship Risk (CRR)
  - The risk that a Customer's Lifetime Value will be negatively impacted by an event
- Customer Relationship Risk Management (CRRM)
  - The processes used to identify, assess, prioritize, and remediate CRR.

Define Risk Approach

- Identify a Risk Management Methodology
  - CSEC/RCMP HTRA (Canada)
  - NIST 800-30 Risk Management Guide for Information Technology (USA)
  - CRAMM (UK)
  - OCTAVE (cert.org)
- Identify the acceptable level of Risk tolerance
  - “Our organization will remediate all identified risks with a risk score of xyz or higher using the abc risk management methodology” signed CEO

Identify the Risks

- Identify the Assets
  - Relationship between your organization and your customers
- Identify the threats
  - Client facing staff antagonize the client
  - Client is unable to reach a contact point at the organization
  - Service delivered to client does not meet the client's expectations

Identify the Risks con't

- Identify the vulnerabilities to those threats
  - Client facing staff lack the required people skills
  - Client facing staff do not have access to information required to satisfy client demands
  - Client facing staff have a language & cultural barrier to overcome
  - Inbound calls frequently exceed call capacity
  - The SPAM filter habitually eats important emails
  - Service sold to the client was not defined well enough

Analyze & Evaluate the Risk

- Identify the business impacts to the organization
  - Impact on payment for current goods & services
  - Impact on future or repeat business with same client
  - Impact on new business if client publicizes their dissatisfaction
  - Impact on public and corporate image as negative press circulates

Analyze & Evaluate the Risk

- Assess the likelihood of a CRM breach taking into account the threat, the vulnerabilities, and the currently deployed safeguards and controls
  - Something that happens every day or will likely happen once a week/month/year?
  - Try to use historical data from same organization
  - If available compare with information from comparable organizations in similar industries or markets
- Estimate the level of Risk and assign it a score

Risk Management Options

- Accept
  - If the assigned risk level is below the previously identified level of acceptable risk, no action is required. Accept the risk
- Mitigate
  - If the assigned risk level is above the acceptable risk threshold, then additional controls or safeguards should be deployed to reduce the risk to an acceptable level. Mitigate the risk.

Risk Management Options

- Avoid
  - If no additional safeguards or controls can be deployed, and the business process can be re-architected to remove the component generating the risk, then the component generating risk should be removed, and the risk should be avoided.
- Transfer
  - Customer Relationship Risk cannot be transferred to a third party or hedged with the purchase of insurance or other contracts

Safeguards & Controls

- Security Controls & Safeguards are divided into four categories

- Prevention/Reduction – Deployed pre-breach. Prevents or reduces the likelihood of a threat agent effecting a security breach
  - Example: A lock on a door
- Detection – Detects that a threat agent is committing a security breach
  - Example: A motion detector positioned behind the locked door, and a security camera outside focused on the doorway

Safeguards & Controls con't

- Response – A safeguard usually triggered by a detection-class safeguard. Results in actions taken to minimize or reduce the severity of the security breach
  - Example: An alarm monitoring company dispatching a police officer to the scene after the motion sensor is triggered
- Recovery – A safeguard activated after the security breach. Reduces or mitigates the loss suffered from the security breach
  - Example: Police recover a stolen laptop outfitted with an assisted GPS/phone home safeguard

Recommending Controls

- It is important to have safeguards or controls from each group represented. This supports the “Defence in Depth” or layered concept.
- Examples of controls to mitigate CRR:
  - Prevention/Reduction
    - All potential hires for client facing roles must be interviewed in person, and must complete an aptitude test
    - All new client facing hires must receive orientation training which includes conflict resolution, and how to effectively deal with clients

Recommending Controls

- Detection
  - Communication channels to allow client feedback are present at every stage of the business process
  - Customer satisfaction feedback is proactively sought from the customer after every significant transaction
  - Independent customer satisfaction audits are conducted at regular intervals
- Response
  - Formal response procedures exist, and are documented
  - Metrics are defined, including minimum acceptable response times to resolve CR issues
  - Staff assigned responsibility to resolve customer relations issues are empowered with the authority to resolve those issues with a minimum amount of bureaucracy

Recommending Controls

- Recovery
  - A root cause analysis is performed after each CRM breach, and additional controls, or modifications to the business process are made to prevent a repeat occurrence
  - Feedback is solicited directly from the customer with questions like “What could we have done differently to improve your experience with us?”
  - In cases where CLV is particularly high, a retention program should be developed. The program may have a negative ROI impact in the short term, but provide substantially greater long term ROI

The CRRM Plan

- Cost out all the recommendations from your risk assessment
- If required, do a business case, and financial projections to justify the expenditure on the CRRM Plan to your senior stakeholders.
- Allocate existing budget or acquire approvals for costs
- Take the findings and recommendations from your Risk Assessment and create a plan to implement them
- Get the plan approved and signed off

Executing the Plan & Monitor the CRRM program

- Deploy the controls identified in your CRRM plan
- Assess the effectiveness of the controls through regular audits
- Update and modify the processes to continuously improve them.

Take Away's

- Your relationship with your customers/clients is an asset
- That relationship must be protected
- Security Risk Management processes can be applied to CRM to provide Customer Relations Risk Management (CRRM)

Questions?

Contact Info
Kelly Walsh
Kelly.fc.walsh@wncs.ca
(866)207-0013 x505

Updated copies of this slide presentation will be available for download at www.wncs.ca/presentations.html a week after the conference