Kennesaw State UNIVERSITY®
Coles College of Business

Center for Information Security Education

Dining for Dollars Or, How to Keep Criminals from Feasting on your Cash

Andy Green
Lecturer of Information Security and Assurance,
Assistant Director, Coles Center for Information Security Education

October 19, 2015

Overview

- Food service entities have a need to protect critical information
- Size is a predictor for the threats that are present and the actions that are indicated
- Organizing for information protection
  - InfoSec Governance
  - Policy Development and Policy Management
  - Risk Management to enable informed risk-based decisions.

Every Organization Is At Risk

- Does an organization have computers?
- Are those computers on a network?
- Is that network connected to the Internet?
- Does an organization have employees?
- Does an organization have customers
- If IT is in use, there is risk from information security threats

Scope of Problem

- Information technology (IT)
  - Enables the storage and transportation of information from one business unit to another
  - IT systems can break down
- The concept of computer security has been replaced by the concept of information security
  - Covers a broader range of issues
    - From protection of data to protection of human resources
- Information security is the responsibility of every employee, especially managers

Are Restaurants Special?

- The National Restaurant Association (NRA) notes:
- 70% of dining establishments are single unit
- Criminals target restaurants as easy targets
- New technology is often vulnerable
- As any business, restaurants are required to protect customer (and their own) data

http://www.restaurant.org/Manage-My-Restaurant/Operations/Regulatory-back-office/4-measures-to-protect-your-network-from-hackers

Recent Breaches

- 5/2015
  - Harbortouch POS breached, ~4,200 restaurants impacted
- 1/2015
  - Wingstop announced multiple franchises breached, as far back as 2012
- 1/2015
  - Chick-fil-A announced breach as far back as 2/2013
  - ~9,000 cards

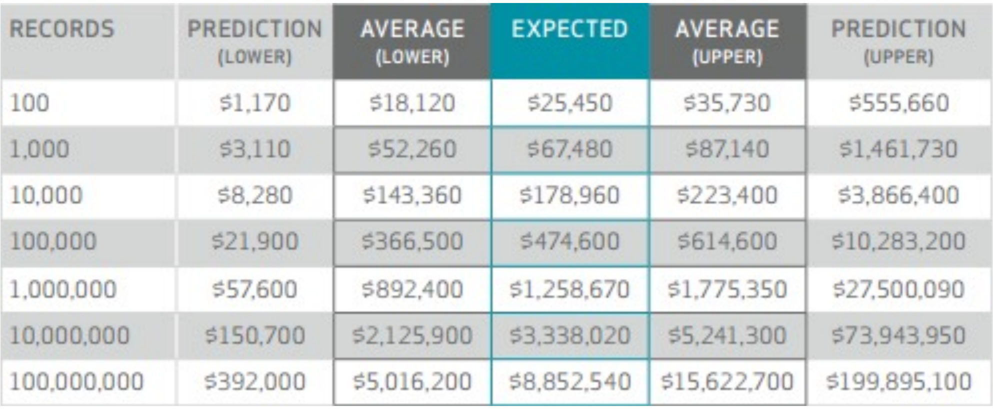
Recent Breaches

- 8/2014
  - PF Chang’s announced breach as far back as 10/2013
  - Thousands of cards
- 10/2014
  - Dairy Queen announced breach of over 400 locations
- 7/2014
  - Jimmy John’s announced breach of over 200 locations

Additional facts to consider

- Verizon Data Breach Investigations Report (DBIR)
  - 28.5% of all confirmed breaches occurred via POS compromise
  - Forecast loss for breach of 1,000 records between $52,000 and $87,000
  - Escalates as record total increases
- Perspective
  - Chick-fil-A (~9000 records) - $468,000 ~ $783,000
  - P.F. Chang’s (~2000 records) - $104,000 ~ $174,000

Anticipated breach losses



RECORDS	PREDICTION (LOWER)	AVERAGE (LOWER)	EXPECTED	AVERAGE (UPPER)	PREDICTION (UPPER)
100	$1,170	$18,120	$25,450	$35,730	$555,660
1,000	$3,110	$52,260	$67,480	$87,140	$1,461,730
10,000	$8,280	$143,360	$178,960	$223,400	$3,866,400
100,000	$21,900	$366,500	$474,600	$614,600	$10,283,200
1,000,000	$57,600	$892,400	$1,258,670	$1,775,350	$27,500,090
10,000,000	$150,700	$2,125,900	$3,338,020	$5,241,300	$73,943,950
100,000,000	$392,000	$5,016,200	$8,852,540	$15,622,700	$199,895,100

2015 Verizon DBIR report

But wait, there’s more!

- Volunteer Voyages
  - Debit card tied to business checking account was compromised, lost ~$14,000
- Wright Hotels
  - Fraudulent transfers from checking account to Chinese account, lost ~$1,000,000
- PATCO Construction
  - Fraudulent transfers from checking account
  - Lost ~$545,000

But wait, there’s more!

- In all cases, banks refused to make restitution
- Commercial accounts are treated differently than individual accounts
  - Consumer accounts protected by Reg E
  - Business accounts held to Uniform Commercial Code (UCC) standard of “reasonable” standard of security offered by bank

http://www.npr.org/sections/alltechconsidered/2015/09/15/440252972/when-cyber-fraud-hits-businesses-banks-may-not-offer-protection

http://krebsonsecurity.com/2015/08/cyberheist-victim-trades-smokes-for-cash/#more-31926

6 Things Each Restaurant Must Do

- National Restaurant Association (NRA) Measures to protect your restaurant
  - Network defense with basic firewall
  - Regular scanning
  - Limit remote access
  - Credit card hygiene
  - Segment your network
  - Keep systems updated and stay engaged with your providers

Protecting your operating accounts

- Dedicated system for online banking
  - NO other activity allowed – Email, web, video, music
  - Consider a “Live CD” option
- Require multi-factor authentication
- Instruct bank to require real-person verification of wire transfers
- Do not use a debit card tied to operating accounts
- Separation of duties
- Audits

Size as a Factor

- Large and Very-large restaurant organizations should be managed as any other business with regard to information security
- Small and Very-small restaurant organizations have few options except to limit risk and try to manage growth to avoid growth induced lapses
- The following remarks are targeted at the middle-sized organizations

Threats

- There are many threats that create a risk that you might suffer a loss.
- Many of these threats are things you may be familiar with:
  - Market risk
  - Financial risk
  - Casualty risk
- You may not be familiar with all the Information Security threats that can cause risk

Managing Risk

- We manage risk using:
  - **G**overnance
  - **R**isk management processes
  - **C**ompliance to regulation
- This is accomplished by applying *controls:*
  - Controls are ways to limit risk
- Continue to work on reducing risk until the leftover risk, called residual risk, is lowered to match organizational expectations, called risk appetite

The real solution

- The real solution to information security risk is in the systematic, top-down application of GRC:
- Governance
  - Create a management mindset and organizational culture that results in lower risk
- Risk Management
  - Application of a methodology to thoughtfully reduce risk while balancing availability needs against risk control needs
- Compliance
  - Meeting regulatory demands, industry benchmarks, or internal baselines

What’s New?

- There are not really any new threats, just new vulnerabilities, exploits, and motivations
- Vulnerabilities are announced every day, usually when an exploit becomes available
- The biggest risk is from *zero-day* exploits
- We do see an evolution in the motivation of the attackers

Restaurant Infosec Resources

- Help is available
  - Trade Associations like NRA
  - SBDC events and outreach
  - Consultants and Contractors

Thank you for your time and attention!

Andy Green, MSIS

Assistant Director – Operations

Center for Information Security Education

agreen57@kennesaw.edu