THE POWER OF BEING UNDERSTOOD

AUDIT | TAX | CONSULTING
SECURITY TRENDS FOR CONSUMER PRODUCTS COMPANIES

April 19, 2017
RSM’s consumer products and retail focus

• RSM US LLP serves over 3,600 consumer products companies from across the country

• We have companies across the country from apparel designers to large retailers and everywhere in between. We have specialty practices focused on fashion and home furnishings, health and beauty, food & beverage, retail and other consumer products sectors.

• To sign up for our monthly retail industry commentary or learn more about our industry focus, visit our website at

• For more information on risk advisory services:
  http://rsmus.com/riskadvisory

• To subscribe to RSM communications:
  http://response.rsmus.com/RSMpreferencecenter

Carol Lapidus
Assurance Partner
National Consumer Products Industry Leader
212. 372.1272
carol.lapidus@rsmus.com
Agenda

• Statistics and Insurance
• Regulatory and Standards Changes
  – PCI
  – GDPR
• Threat Updates
  – Ransomware
  – Ransom “Mega” DDoS
SECURITY STATISTICS
Security Statistics
Quick Hits

KEY FINDINGS

Breaches are not just for the Fortune 500 companies anymore.

The majority (87%) of claims submitted for this study are for organizations with revenues less than $2B.

Breaches can be very costly, no matter how large or small an organization may be.

In our dataset, breaches with total costs greater than $5M occurred in organizations of all sizes except Mid Rev ($2–10B).

The numbers of records lost can be large, no matter how large or small an organization may be.

Our dataset contains breaches of 1M or more records occurring in organizations of all sizes, except Mega Revenue (>100B).

The average number of records lost was 2.04 million. The median number of records lost was 1,339.

The greatest numbers of exposed records occurred in the Financial Services (78M records) sector, followed by Retail (56M records).
Third parties accounted for 13% of the claims.

There was insider involvement in 30% of the claims.
- This includes mistakes and errors
- Also includes rogue employees and purposeful malicious actions

The average cost for legal settlement was $815k.

75% of costs were tied to Crisis Services.
- Incident Response, hotlines, notifications, etc.
- The costs were compounded by the organizations not having robust incident response plans

Ransomware average costs were $32k but raising quickly.

The average claim payout was $495K.
The linkage has broken between the cost of a breach being tied to the number of records that were exposed.
Security Statistics
Claims Payouts – Trend Continues

Compiled from:
- NetDiligence/RSM 2015 & 2016 Annual Cyber Claims Study

Average Claim Payout

- 2011: $2,425,754
- 2012: $3,606,000
- 2013: $954,253
- 2014: $733,109
- 2015: $673,767

Security Statistics
Claims Payouts – Trend Continues

©2017 RSM US LLP. All Rights Reserved.
Cyber Liability Insurance

• The last line of defense

• Do you have cyber insurance?
  – Don’t count on it being covered under your general policy

• Do they cover the common costs?

• Are the sub-limits reasonable?

• Have you complied with all of the covenants?
  – Mapped security policy, IR plan, IR exercise, Security testing, Security monitoring, etc.

• Are your forensic and legal providers approved?
Cyber Liability Insurance

- Insurance: Cover all sources of loss
  - Calculate potential losses
  - Business interruptions
  - Contract violations
  - Value of IP
  - Consultants, forensics, lawyers, recovery costs, man hours
- Insurance: Cover all the event types
  - Malware
  - Ransom
  - Social Engineering
  - Employee mistake
  - Etc.
REGULATORY AND STANDARD CHANGES
PCI and GDPR
 PCI Data Security Standard Version 3.2 Updates

• The PCI-DSS version 3.2 was published April 2016. This version of the standard will be considered effective immediately.
• Version 3.1 of the PCI-DSS retired on October 31st, 2016.
• After the October 31st date, all ROCs must follow version 3.2 of the PCI-DSS.
• Visa no longer accepts version 3.1 ROCs.
<table>
<thead>
<tr>
<th>LEVEL</th>
<th>Transaction Amounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6 to 20 Million transactions per year</td>
</tr>
<tr>
<td>2</td>
<td>1 to 6 Million transactions per year</td>
</tr>
<tr>
<td>3</td>
<td>20 thousand to 1 Million transactions per year</td>
</tr>
<tr>
<td>4</td>
<td>Any merchant with 20 thousand transactions or less per year</td>
</tr>
</tbody>
</table>
PCI DSS 3.2 updates

• Verification that policies and procedures are in place and operating effectiveness of those policies are part of the duties of the QSA

• Removal of “strong” or “secure” language around protocol examples provided in a number of requirements, since these may change at anytime (Requirement 1.1.6)

• Selected business-as-usual and governance principles may be required for certain organizations as defined in the Designated Entities Supplemental Validation (DESV) (Appendix A3)
PCI DSS 3.2 updates

- While some requirements will be considered “best practice” until January 31 2018, such extension is not intended to delay migrations.
- For example to secure versions of SSL or multi-factor authentication implementations, merchants will still have to demonstrate how they are addressing the risks represented by weak implementations of SSL or authentication methods that could be part of their cardholder data environment.
- Clarified correct term is multi-factor authentication (rather than two-factor authentication) as two or more factors may be used.
PCI DSS 3.2 updates

• Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication (8.3) (best practice until January 31, 2018).

• PCI DSS will incorporate two new appendices in the standard that were previously separate supplemental documents:
  • Appendix A2—Additional PCI DSS requirements for entities using SSL/ Early TLS.
  • Appendix A3—Designated entities supplemental validation (DESV).
What is GDPR?

• European Union General Data Protection Regulation - “EU GDPR.”

• New data protection law adopted by the EU in April 2016 intend to bolster data protections for EU residents.

• Companies, government agencies, and non-profits interacting with EU residents have until May 2018 to comply.
Scope

• To determine if GDPR affects an organization, they need to answer any of the following:
  – Do they offer goods and services to people in the European Union?
  – Do they have third parties which store or send data to the EU?
  – Do they collect or analyze the data of EU residents?

• “Data” means: “anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address”.

• Essentially, if you touch any data from the EU then GDPR most likely applies to you.
5 Big Concepts to Understand

1) Accountability
   - Appoint Data Protection Officer if storing or processing data on more than 5,000 EU residents

2) Consent
   - Must be explicit “opt-in”, most “opt-out” types not acceptable
   - Usage of data must be explicit including access by 3rd parties

3) Right to be Forgotten
   - The most difficult to deal with for many organizations

4) Portability

5) Breach Notification
   - 72 hours to notify EU authorities
The Penalty of Non-Compliance

• If organizations do not comply, they face a maximum fine of:

4% of their total revenue  
OR  
€20 million Euros

...whichever is higher

• Organizations can be fined if their outsourced data hosting/processing/etc. is breached

• Note: “Other types of breaches” can be fined at €10 million or 2%
THREAT UPDATES
Major Concept:

• The core of the issue is the attacker denying access to some resource that you require and forcing you to pay to regain access

• Far, far less technically demanding than other types of hacking, so it allows a lower-skilled attacker to succeed at the basic versions of it

• However, advanced attackers have come out with a new wave of extremely dangerous variants of the attack
Major Concept:

• What is your current ability to pay?
• Essentially all payments are required to be in BitCoin
• The major issue for most clients hasn’t been the actual ransom amount, though that is quickly becoming material, is how quickly the client can gain access to the BitCoin needed to pay
• On the major, fairly legitimate exchanges it is the same as opening a bank account
• Validation of identity, 5-7 days to open the account
Threat Overview

• Quiz Time!
  − What are the differences between these three items?
  1. Locky: Common ransomware. Pay or don’t pay.
  2. Ranscam/Fakelock: Completely fake. Uses the pop-up to scare victims into paying but actually does nothing.
  3. Le Chiffre: New variant. It is MANUALLY DEPLOYED.

• Those bold letters should be considered a hint.

• What does it mean if you encounter this malware in your environment?

Attention!

Your important files (photos, videos, documents, archives, databases, backups, etc.) which were crypt with the strongest military cipher RSA1024 and AES. No one can’t help you to restore files without our decoder. Photorec, Ransom Decryptor, etc repair tools are useless and can destroy your files irreversibly. If you want to restore files – send e-mail to decrypt.myfiles@gmail.com with the file _secret_code.txt_ and 1-2 encrypted files less than 5 MB as *.doc*, *.xls*, .jpg, but not database (*900* *001* etc.). Please use public mail yahoo or gmail.

You will receive decrypted samples and our conditions how you’ll get the decoder. Follow the instructions to send payment.

P.S. Remember, we are not scammers. We don’t need your files. If you want, you can get a decryptor for free after 6 month. Just send a request immediately after infection. All data will be restored absolutely. Your warranty - decrypted samples.

Secret code:

IGBDMKXPbVbPbrRzqgNIsz9g9uW1L5K2TEAKuA97l2DFlH-b0R9da53DcFSe8JO6lUGmED1VXJzbwATYMNk-FgkuwswW0dq8R0FGvLN
Threat Overview

Ransom

• DDoS Style

• Basically throwing so much traffic at your network/systems/applications that they cannot function

• Cyber equivalent of a traffic jam

So, it’s your turn! All servers under DDoS attack unless you pay us. Ygr0

Please note that it will cost you 250 USD, so we are serious.

We are aware that you probably don’t have 250 USD, so we will give you 24 hours to get it and pay. If you don’t, we will attack your bitcoin address, you don’t even need to pay 250 USD, so we are cheap, and we do it.

IMPORTANT: You don’t even have to pay us. We’ll just keep attacking. We say it because big companies always pay, they always pay, and that is true. If you say you don’t have 250 USD, we will wait 24 hours, and if you don’t, we won’t stop and we’ll take 100 BTC.

DD4BC attacks have increased dramatically over the last few months. Source: Akamai
Threat Overview

• Those numbers were from 2015
• The FBI helpfully broke up that specific hacking crew
• Guess what? They had kids!
• And they don't like being tattled on!
• And they are growing up!

TL;DR version

If they target your organization, there is essentially zero chance any DDoS mitigation product can survive the event.

The decision is to pay, fail over to DR/BC plans, or wait.

What do you do?
Questions:

• Do you have some basic playbook laying out your response and investigation to ransom issues?
  - Moderate DDoS
  - Large scale DDoS
  - Ransomware of varying complexity on systems of varying value and sensitivity

• Can you respond rapidly?

• Does your insurance cover the expenses?
  - That sure changes the math, right?
  - We’ve seen ransoms as high as $250k