Getting Data Breach Right
Lessons Learned from Fighting in the Cyber Trenches

John Ansbach, JD, CIPP-US
Vice President, Engagement Management
Top 10 Breaches through July 2018 exposed roughly 1.9 billion records
Data breach continues to represent one of the most significant risks to enterprise, regardless of organizational type, industry, size or profit motive.
The question is, how should we respond when these breaches occur?
Agenda

- Landscape
- What We're Seeing
- Observations & Lessons
- Recommendations for Response
Landscape
Over 2,300 Data Breaches Disclosed So Far In 2018, Exposing Over 2.6 Billion Records

AUGUST 15, 2018 BY RBS

Risk Based Security today announced the release of its Mid-Year 2018 Data Breach QuickView report, showing there have been 2,308 publicly disclosed data compromise events through June 30th. After a surprising drop in the number of reported data breaches in first quarter, breach activity appears to be returning to a more “normal” pace. At the mid-year point, 2018 closely mirrors 2016’s breach experience but still trails the high water mark set in 2017.

Get Your Copy Of The 2018 MidYear Data Breach QuickView

Key Findings for Mid Year 2018

- 2,308 breaches have been reported through June 30, exposing approximately 2.6 billion records.
- Compared to the midway point in 2017, the number of reported breaches is down from 2,439 breaches and the number of exposed records is down from 6 billion.
- The number of disclosed instances targeting employee W-2 forms remained low, with 42 such breaches reported through Q2 2018 compared to 239 for the same time period 2017.
- The Business sector accounted for 40% of reported breaches, followed by Medical (8.3%), Government (8.2%) and Education (4.5%). Nearly 40% of breached organizations could not be definitively classified.

“After a surprising drop in the number of reported data breaches in first quarter, breach activity appears to be returning to a more “normal” pace.”

Source: Risk Based Security Aug 2018
Annual number of data breaches and records exposed (in millions) in the United States 2005 – Q2 2018

Image via Statista.com.
This statistic presents a ranking of the industries most commonly impacted by cyber attacks worldwide as of September 2017. During the survey, 26 percent of respondents from the energy sector stated that their company had been victim of cyber attacks in the past 12 months.
## Breach Costs

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. average cost of a data breach</td>
<td>$7.91 M</td>
<td>$7.3 M</td>
</tr>
<tr>
<td>World average cost of a data breach</td>
<td>$3.86 M</td>
<td>$3.6 M</td>
</tr>
<tr>
<td>World avg. per capita cost</td>
<td>$148</td>
<td>$141</td>
</tr>
<tr>
<td>(Per capita cost is the avg. cost of a lost or stolen record compromised in a data breach)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Per capita cost in the U.S.</td>
<td>$233</td>
<td>(highest; was $225)</td>
</tr>
</tbody>
</table>
The cybercrime cost prediction includes damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.
What We’re Seeing
Web App attacks up 69%, US main source of cyber attacks

Nov 29, 2017
NEWS by Grace Johansson

Web application attacks have grown 69 percent compared to Q3 2016, up 30 percent on the previous quarter according to the Akamai Q3 State of the Internet Security Report.
What We're Seeing – Web App Attacks

+ A lot of companies digitizing their approach to business
  - Effort to engage customers via web portals

+ Especially in ‘blue collar,’ ‘traditional’ enterprise
  - Shipping and logistics
  - Energy
  - Manufacturing

+ Insecure, web-facing applications, portals, devices are a result of business getting ahead of security
Example Case 1 – Web App Attack

- 2 days later, attackers conducted recon from a TOR node IP address

- The next day, attacker comes back, logs in from TOR node, and begins downloading documents using credentials compromised from SQL attack

- Company takes the web portal offline, engages outside security firm

- Krebs publishes post on the attack

- NY Times Article about the Company
- Attacker domain registered

- 2 days after that, attacker begins a sustained SQL injection attack against company from a Netherlands hosting co

- Day after that, attacker sends stolen data to media outlet, who contacts the co and publishes the attack
What We're Seeing

Inside Dropbox and Microsoft Office phishing attacks | Salted Hash, Ep. SC03

In this week's video, we look at a Microsoft Office phishing attack that leverages Dropbox as the lure.

O365 BEC attacks

Dropbox file share

Office 365 ‘account is full’

Account takeover
What We're Seeing – O365 BEC

+ High level execs targeted
+ Money is the motivation
  − Still have to deal with access, exfiltration, notification
+ Nigerian IP addresses
+ Across industries
  − Financial
  − Shipping and logistics
  − Energy
  − Manufacturing
  − Construction
+ Heavy use and manipulation of rules to effectuate fraud and mask activity
Example Case 2 – O365 BEC

Construction company executive targeted by phishing email

Hovering over the “View Shared Document” graphic in the e-mail revealed a hyperlink, which is a link shortener service that would then redirect the clicker to (in this case) a reputed credential phishing site URL.

Once at the site, unsuspecting co exec entered credentials, allowing attackers to subsequently wire $670K out of employee pension fund
Note: even after the root cause was identified and remediated, investigation revealed that attacker set up a forwarding rule.

Result was exfiltration of sensitive company data (victim had PHI and PII in his email traffic).

Also evidence of PST file download, requiring extensive forensic analysis of PST contents for breach notification.
Example Case 3 – O365 BEC

Appears to come from Microsoft Support Team

“ACTION REQUIRED”

“(7) incoming messages failed to deliver”

High importance

Inbox at 95%

“To free up some space right now, we’ve simplified the process for you. Click below.”
Example Case 3 – O365 BEC

Resulted in a fraudulent wire transfer of $1.7M

Extensive use of rules (forwarding and otherwise) to push and mask communication

Additional forensic review required to determine exfiltration
What We're Seeing

Shipping company’s networks in the Americas crippled by ransomware attack

China’s state-owned COSCO gives customers Yahoo addresses to use in the meantime.

DAN GOODIN - 7/26/2018, 4:25 PM

Ransomware attacks

Large and small co

Advance attack & recon work resulting in backup encryption & deletion

Not just drive-by; active attacker in the environment
What We're Seeing – Ransomware

+ SamSam

+ Bitpaymer

+ Biggest change we're seeing is the advanced work

+ Deleting or encrypting files ahead of the ransom


What happened to your files?
All your files encrypted with RSA-2048 encryption, For more information search in Google 'RSA Encryption'.

How to recover files?
RSA is an asymmetric cryptographic algorithm, You need one key for encryption and one key for decryption. So you need Private key to recover your files. It’s not possible to recover your files without private key.

How to get private key?
You can get your private key in 3 easy steps:
Step 1: You must send us 0.7 BitCoin for each affected PC OR 3 BitCoins to receive ALL Private Keys for ALL PCs.
Step 2: After you send us 0.7 BitCoin, Leave a comment on our site with this detail: Just write Your Host Name is:

Step 3: We will reply to your comment with a decryption software, You should run it on your affected PC and pay for all affected PCs.

Our Site Address: http://jcm15n4clmvgtyx5.onion/familiarisingly/
Our BitCoin Address: 1MddNhqeR4fJxeg2t5ywdjbdAQpslWNpKhmFR

If you send us 3 BitCoins For all PCs, Leave a comment on our site with this detail: Just write ‘For All PCs.
(Also if you want pay for 'all affected PC's' You can pay 1.5 BitCoins to receive half of keys(randomly) and others half by your comment)

How To Access To Our Site
For access to our site you must install Tor browser and enter our site URL in your tor browser.
You can download tor browser from https://www.torproject.org/download/download.html.en
For more information please search in Google 'How to access onion sites'

# Test Decryption #

If you are worry that you don't get your keys after you paid, You can get one key for free on your choice(except important servers), Tell us your PC id and we will give you one free key.
Also you can get some single key and if all single BTC tah you paid reached to all keys price you will get all keys.
Anyway be sure that you will get all your keys if you paid for them and we don’t want damage our reliability.
With buying the first key you will find that we are honest.
Example Case 4 – SamSam Ransomware

+ Early morning hours ransomware attack

+ Company’s network and customer facing portals taken down (over 75 servers)

+ Investigation revealed prior recon attack via Remote Desktop Protocol (RDP)

+ Brute force password cracking (poor password hygiene) also likely

+ Payment of ransom selected to avoid significant data loss; initial payment produced valid random decryption keys
What We're Seeing

Cryptojacking attacks: One in three organisations say they've been hit with mining malware

Cryptocurrency-generating malware has been on a rampage this year - but some organisations still haven't done much to defend against it.


Web crooks are making money by forcing PCs and other devices to mine cryptocurrency for them, according to new research.

Cryptojacking Attacks

Targeting companies with large scale infrastructure and significant computing power
Example Case 5 – Cryptojacking a Major University

+ Major university system
+ One of the top 10 most powerful supercomputers in the world (according to TOP500 Supercomputer Sites, which ranks the 500 most powerful computer systems in the world)
+ Malware coopted processing from 10pm – 6am local time for the purpose of mining cryptocurrency
+ The timing of the effort kept users from noticing a drop in performance
+ Before it was discovered and disabled, the attackers were able to mine a significant amount of Monero (1XMR = $99 as of 8/20/2018)
+ Even after remediation, still questions as to data access and exfiltration, breach notification
Observations & Lessons - People

+ C-Level engagement matters
  - Micromanagement v. absenteeism

+ Talent level of infosec personnel matters

+ Pressure
  - From people above, from people who own (parent cos, PE owners)
  - Watch for CYA, competing agendas

+ Organization
  - How well is your group organized?

+ Communication
Observations & Lessons - Processes

+ Internal notification
  - What is your process for discovery, internal notification, plan execution

+ What is the plan for engaging partners?
  - Outside counsel, forensic providers, comms firms, insurance

+ What is your process for onboarding a forensic provider?
  - Like jumping onto a moving train; requires patience during a time when time is critical
  - Also, IT may not welcome the help

+ What is your process for supporting an investigation?
  - Do you have logging?
What controls do you have in place to preserve critical data?

Case example:
- In ransomware example previously, company not only disconnected file servers, they powered them down
- Result was loss of virtual memory and logs that could have helped in investigation and getting company back up and running
- Company had no established controls in place to preserve data critical to restart or investigation

Lesson
- Practice these events
- Tabletop of a ransomware attack would have prepared this company
- IR playbook developed in concert with forensic and legal counsel would have dramatically shortened response timeline
Recommendations
Recommendations - Pre-Breach

+ Before a breach occurs:
  • Establish an actionable, up-to-date incident response (IR) plan
  
  • Tabletop it, run sims on breaches that your org is most likely to experience
  
  • Working with IT, develop detailed data loss prevention (DLP), disaster recovery (DR) and business continuity plans (BCP)
Recommendations - Pre-Breach

- Negotiate an **IR retainer agreement** with a forensic provider, get to know them
- Select a law firm partner
- Establish a relationship with a PR firm
- Get to know law enforcement
Recommendations, When a Breach Occurs

+ Collaboration
  - General Counsel colleague of mine advised of a breach they had, in which IT didn’t notify Legal
  - No harm in over notifying folks
    - FYI, we’ve had an incident, here is what we know, what don’t, etc.

+ Organization
  - Most IR’s we come into begin with chaos and are worked into order
  - Have to get DB team, infosec team, ops, comms and IT…all on the same page
Recommendations, When a Breach Occurs

+ Leadership
  - Under pressure
  - Multiple pushes and pulls
  - Multiple unknowns
  - Jobs on the line
Top 5
Top 5 Do’s

1. Avoid the blame game

2. Get communication right (not too much, not too little…)

3. Manage and lead (can’t be always on for 3 weeks)

4. Get the right partners (law firms, forensics, comms, insurance)

5. Practice (tabletop done right) (will surface issues related to network segmentation, backup and DR, cryptocurrency purchasing, etc)