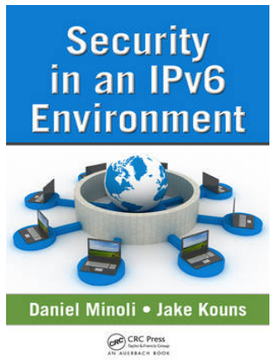
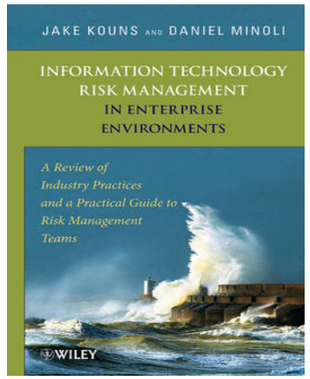
Jake Kouns, CISO
Risk Based Security

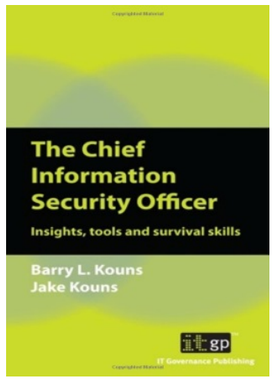
Integration of Cyber Insurance Into A Risk Management Program

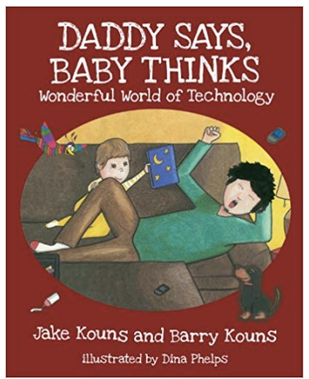
@jkouns

- CISO at Risk Based Security
- Founder of RVAsec (May 5-6, 2019)
- Previous OSVDB & DataLossDB
- Cyber Liability Insurance “Expert”
- Spoke at DHS & Pentagon about Cyber Insurance
- Vulnerability Intelligence & Vendor Risk Ratings
- Spoke at Black Hat, DEF CON, RSA, FIRST, InfoSecWorld, DerbyCon and many more!
- Colts, Capitals, Orioles Fan (yes, sportsball!)





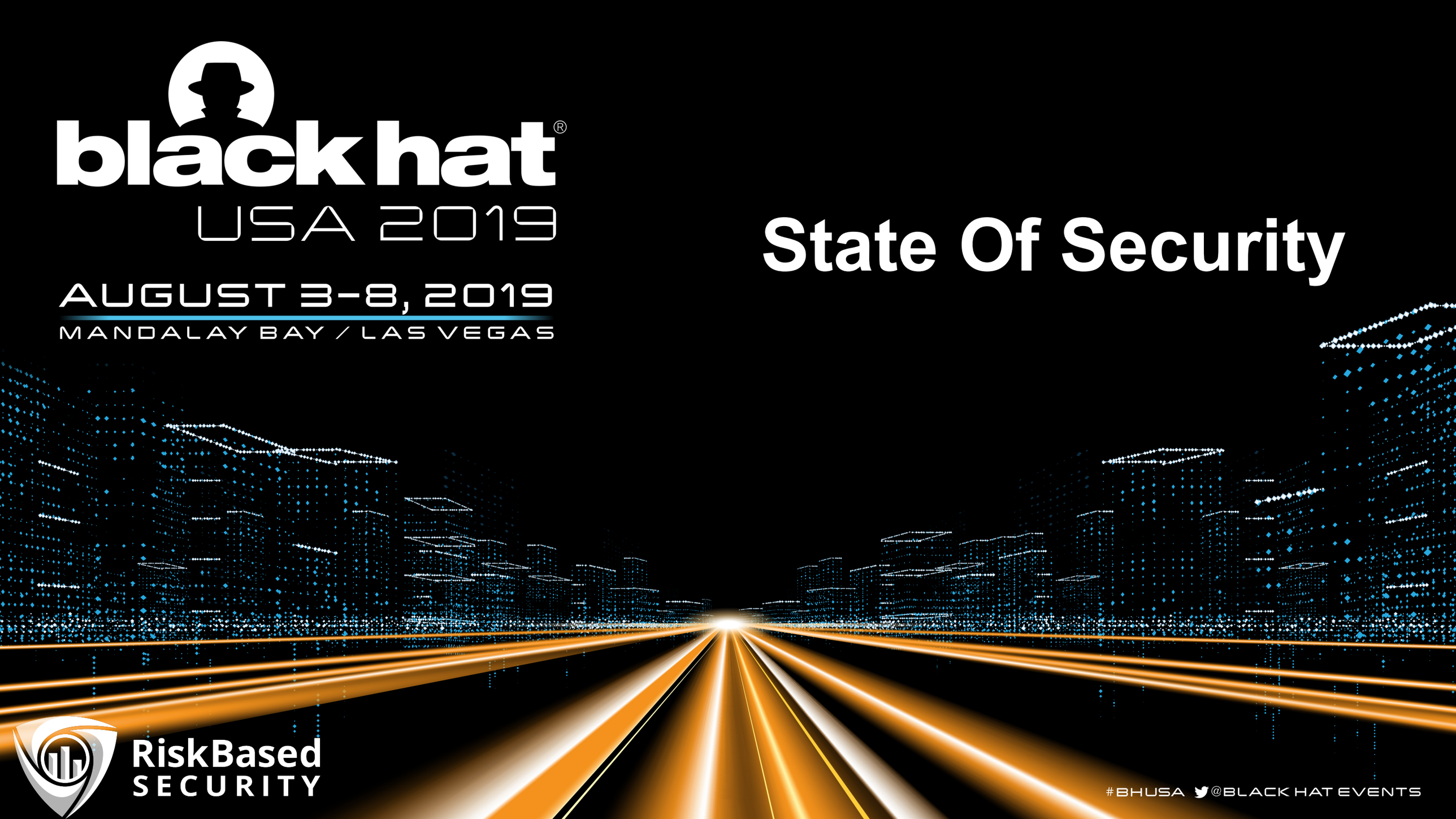


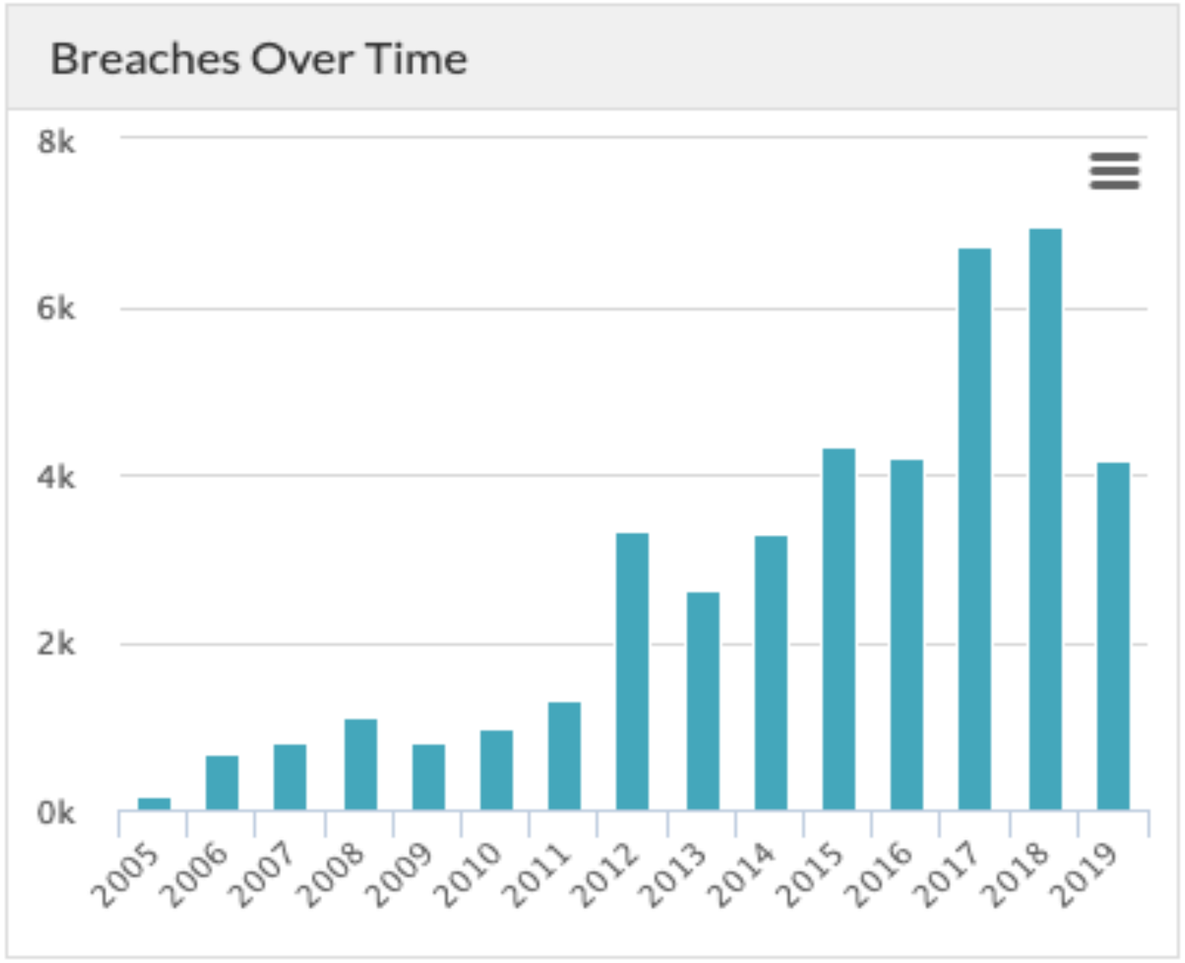


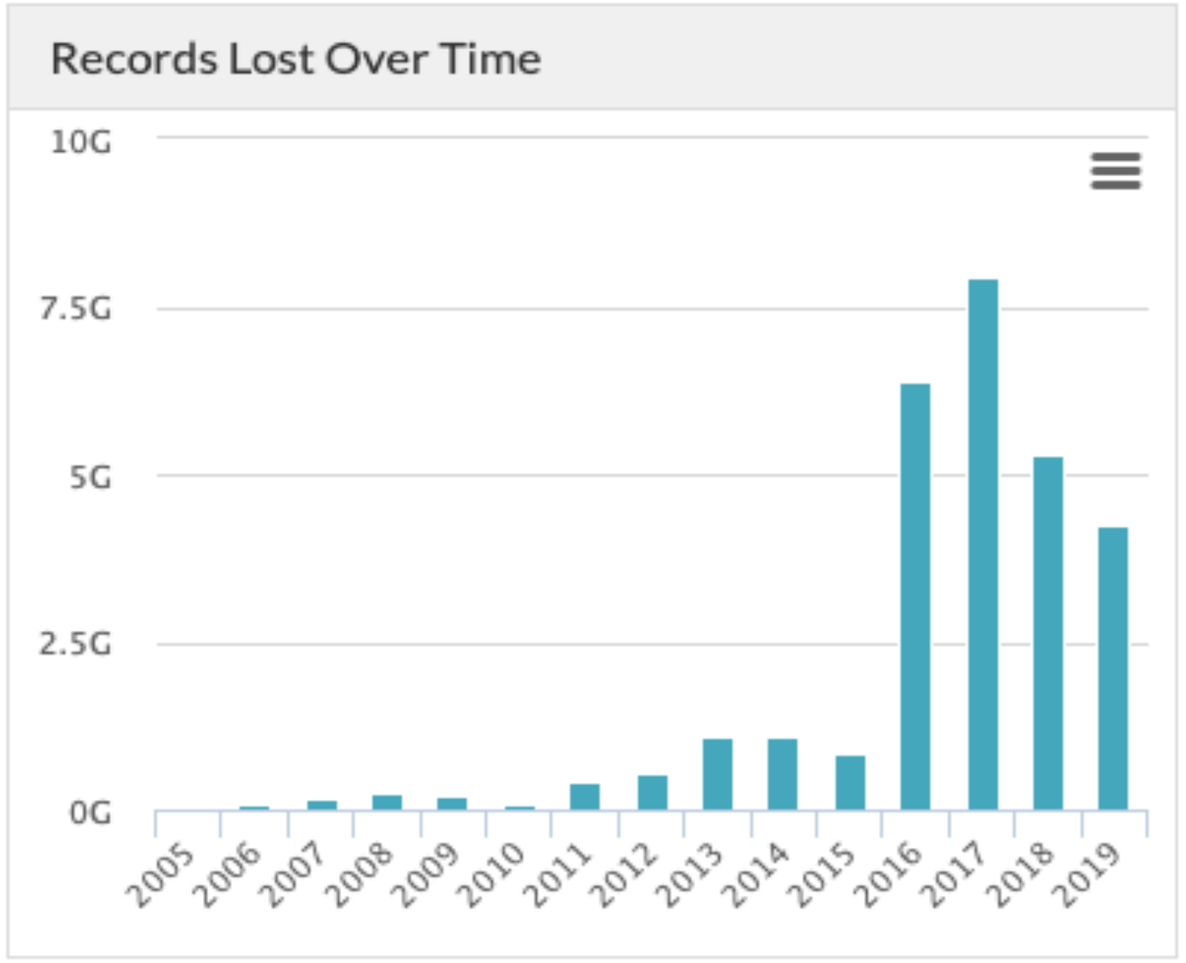
April 2010 Issue of SCMagazine

RiskBased SECURITY

BLACK HAT EVENTS


black hat
USA 2019
AUGUST 3–8, 2019
MANDALAY BAY / LAS VEGAS
State Of Security
RiskBased
SECURITY
#BHUSA @BLACK HAT EVENTS





Source: CyberRiskAnalytics.com

2019 Mid Year Breach Analysis

- 3,813 breaches were reported
- 4.1 billion records exposed
- Compared to Midyear 2018:
  - The number of reported breaches was up 54%
  - The number of exposed records was up 52%

On track for yet another worst year ever…

Data Breach – Ticking Time Bomb?

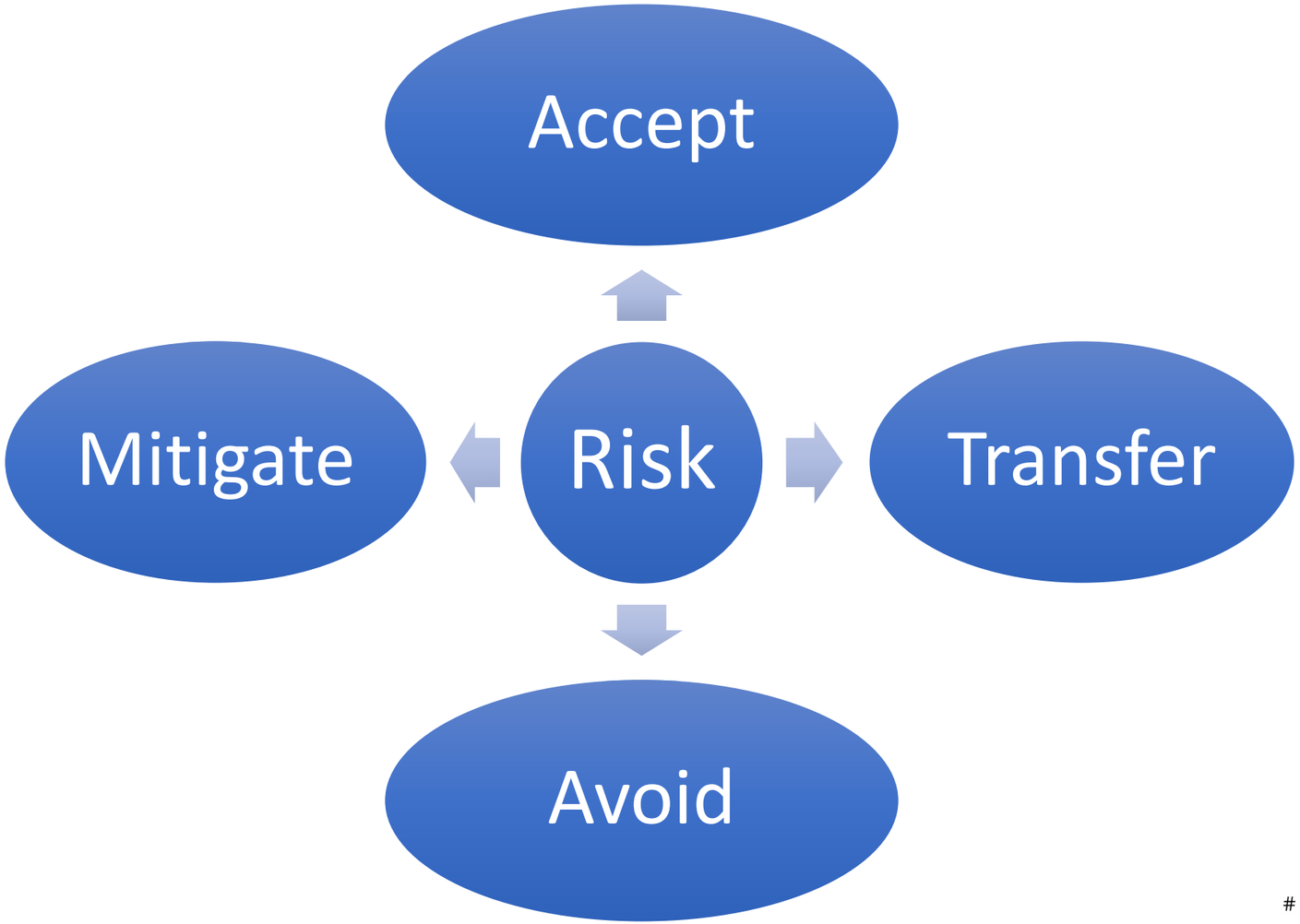
Only a matter of when for most organizations?

Data Breach – How Much Does It Cost?

Data Breaches cost organizations money!


black hat
USA 2019
AUGUST 3–8, 2019
MANDALAY BAY / LAS VEGAS
Risk Management &
Insurance
RiskBased
SECURITY
#BHUSA @BLACK HAT EVENTS

Reality of Risk



Transfer Options

- Outsourcing
  - Contracts & Agreements
    - Insurance

- Insurance is purchased for numerous reasons:
  - Reducing liability
  - Loss recovery
  - Legal requirements
  - Securing loans and/or investments
  - Improving business image and stability
  - Peace of mind
- Typically purchased for most valuable assets

Insurance Coverage

Insurance Coverage

Insurance Coverage

Insurance Coverage

Cyber Insurance Coverage

Why ~~do people hate~~ haven't more organizations bought Cyber Insurance?

- They have "unbreakable" security controls?
- They think the coverage won't last or respond?
- They don't believe its a good spend of budget?
- They are not aware of the market?
- Something else?
- Perhaps, organizations don't truly understand it?

Trust The Salesman!

Is The Bad Reputation Well Deserved?

Is The Bad Reputation Well Deserved?

< Cyber-insurance shock: Zurich refuses to foot NotPetya ransomware clean-up bill – and claims it's 'an act of war'

US snack food giant Mondelez is suing its insurance company for $100m after its claim for cleaning up a massive NotPetya ransomware infection was rejected – for being "an act of war" and therefore not covered under its policy. Zurich American Insurance Company has refused to pay out on a Mondelez policy that explicitly stated …

PF Chang's Loss Highlights Common Holes In Cyber Coverage

Law360, Los Angeles (June 8, 2016, 8:54 PM EDT) -- An Arizona federal court's recent ruling that P. F. Chang's isn't covered under a cyberinsurance policy for assessments that


black hat
USA 2019
AUGUST 3–8, 2019
MANDALAY BAY / LAS VEGAS
Cyber Liability Insurance
(quick recap)
RiskBased
SECURITY
#BHUSA @BLACK HAT EVENTS

Many Names, Many Carriers

- Cyber Liability
- Privacy Injury Liability
- Network Security Liability
- Data Privacy
- Theft of Digital Identification
- Cyber Extortion
- Internet Liability

Little Commonality

≠

First Party

Pays to fix the things we own when damaged

Third Party

Pays others when our actions (or inaction) causes harm

As a result of a security event including data breach or compromise

Third Party

First Party

 Michael Jastremski

Why does this matter?

Because it means organizations can buy a cyber policy that can cover *both*

- Security event recovery costs

&

- Protection from lawsuits arising out of a data compromise

It is important to identify the types of incidents that may impact you!

Breach Notice Compliance

- Forensics
- Legal fees
- Mailings
- Credit Monitoring
- Identity protection

Liability

- Defense costs
- Settlements
- Responding to regulatory investigations
- Costs to reissues credit or debit cards
- Website & Social Media

Other 1st Party

- System Restoration & Extra Expense
- Payment of Extortion Demands & Lost Business

Not all cyber insurance policies are the same!

As helpful as some of these policies can be, expect some things not to be covered..

Reputation Damage

Regular maintenance **Upgrades** **Fixes**

The economic value of data

Data or systems in the care, custody or control of others

Coverage – Not So Common Exclusions

- Failure to encrypt data (mobile devices)
- Failure to maintain or take reasonable steps to maintain security
- Coverage limited to web site and Internet activities only
- Widespread virus / Spyware
- Failure to comply with PCI standards
- Wireless
- Cloud / SaaS
- Business Income Loss
- Contingent Business Interruption (Contingent BI)

Not all cyber insurance policies are the same!

Yes, you need to read the policy!

Or… hire someone to do it for you =)

black hat USA 2019

AUGUST 3–8, 2019

MANDALAY BAY / LAS VEGAS

Integrating Cyber Liability Insurance

RiskBased SECURITY

#BHUSA @BLACK HAT EVENTS

Integrating Insurance

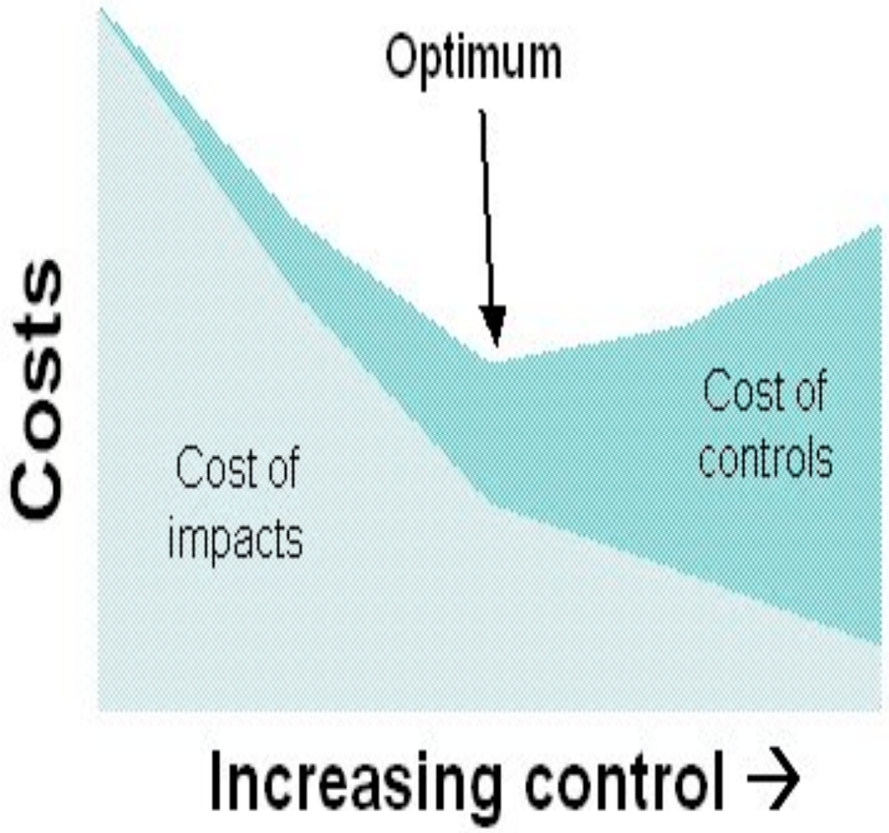
- Executives understand risk:
  - Avoid, Mitigate, Accept and Transfer
- Organizations understand the need to protect their most important assets and transfer risk already:
  - Property (Buildings)
  - Casualty Coverage (Accidents)
  - Employment Practices Liability & Workers Comp (People)
  - Professional Liability - Errors and Omissions

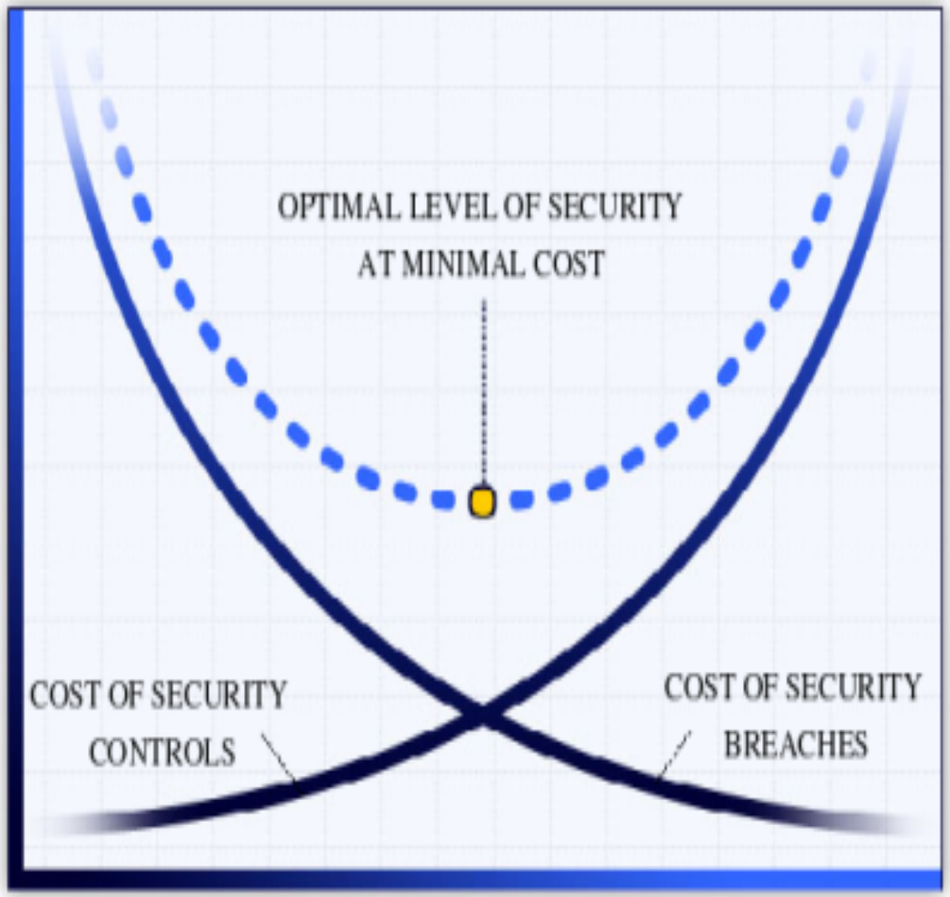
Integrating Insurance – Perfect Security

Integrating Insurance – Law of Diminishing Returns

$$\frac{1}{X}\sum_{i=1}^{x}\frac{1}{2^{i-1}} = D$$

Integrating Insurance – Optimal Security





- Let us estimate costs for a security program for a small business (Approximately $2-5M revenue)
  - Security Staff
  - Security Software / Hardware
    - Antivirus, Encryption, Firewall, IDS, DLP, Compliance, Scanners, etc.
  - Security Consulting
    - External Vuln Scans, Pen Tests, PCI compliance, Legal, Awareness, etc.

Integrating Insurance

- For sake of argument……
- Lets say it costs a business with $2-5M in revenues spends approximately $200,000/per year on security
- Not including initial investment costs
- This estimate is extremely low if they are to implement proper security
- Should they be spending more?
- Does this ensure that they won’t have a breach?

Integrating Insurance

- Typical costs for Cyber Insurance are currently extremely reasonable
- Minimum premiums can be < $1,000 for $1M in coverage
- Includes many Risk Management Services
- Pricing can change based on industry and controls
- Many smaller companies confused by security and are not yet doing anything

Integrating Insurance

- Larger organizations can also get Cyber Insurance for a reasonable cost
- Large hospital with $2B in revenues premium estimates:
  - <$100,000 for $1M in coverage
  - <$200,000 for $5M in coverage
- Limits are available up to $100M from a single carrier
  - But large large towers can be built upwards of $750M (called Excess)
- Pricing can change based on industry & controls
- Larger organizations don’t typically use Risk Management Services, but they can utilize service rates

Not all cyber insurance policies are the same!
nor
are they priced the same!

Yes, you need to shop around!

Despite some limitations, there is real value found in these cyber insurance policies.

Cyber Insurance Is Sexy?

Jake's Rejected BlackHat CFP Submission

- 2011 – Rejected
  - Cyber Liability - Who pays when your data goes missing?
- 2012 – Rejected
  - Cyber Liability - Who pays when your data goes missing?
- 2016 – Rejected
  - These Aren't The Incident Response Processes You're Looking For
- 2017 – Rejected
  - PANEL: Cyber Liability Insurance: Misinformation Everywhere!

Cyber Insurance Wasn't Sexy

"I appreciate the need for this talk, but not at Black Hat."

cfp@blackhat.com
to me

Fri, Jun 8, 2012, 10:25 PM

Hello,

Unfortunately we are not able to accept your submission "Cyber Liability Insurance - Who pays when your data goes missing?" for Black Hat USA 2012 CFP at this time.

Accepting presentations [illegible] not like your co[illegible] because there [illegible] three plus events a year. Your content may work better in one of our other conferences. You are welcome to resubmit the presentation for upcoming events when their CFP's open. We will re-evaluate your submission in the context of the event you choose. Being declined once does not necessarily mean your submission will be passed on again.

Please note t[illegible] tough[illegible]

We would still like to have you participate at Black Hat USA 2012 and are offering a 25% off discount of the final registration price at the time you register. This offer is good for online registrations only and may not be combined with any other discounts. If you would like to take advantage of this discount, please email us at cfp@blackhat.com for the appropriate discount code.

Feedback from the reviewers (delegates and review board)

Review Board Member:
I appreciate the need for this talk, but not at Black Hat.

Please respond to this email if you have any questions.

Thank you,
Black Hat Review Board

Interest On The Rise! – Cyber Insurance

Google Trends cyber insurance

Interest over time


black hat
USA 2019
AUGUST 3–8, 2019
MANDALAY BAY / LAS VEGAS
Love It or Hate It:
What You Need
To Know
RiskBased
SECURITY
#BHUSA @BLACK HAT EVENTS

What You Need To Know

- If your organization doesn't have cyber insurance, it will most likely soon!
  - Contractual requirements
- Information Security professionals and responders need to know about cyber insurance
  - Help fill out the applications and ensure proper coverage!
  - Know what cyber insurance will cover!
  - Ensure the requirements of a cyber policies are met to ensure coverage will not be nullified.

black hat USA 2019

What You Need To Know

- Most companies have focused on creating and defining Incident Management teams and processes
- Some organizations had the unfortunate opportunity to test those process and have responded to an incident and/or data breach
- With Cyber Insurance, there are several processes that might need to change
  - Much is based on the specific carrier/policy selected

What You Need To Know – Claims Process

- The claims process, is much like a normal personal insurance policy
- When there is an issue, you need to notify your cyber insurance provider
- From there, they will assign a Claims “adjuster” to your issue
- Based on the situation, the claims process can take several paths

What You Need To Know - Reporting

- Almost all policies have requirements about timely reporting:
  - Within 30 days
  - Within 60 days
  - As soon as practical

- If a data breach happens, and you don't notify the carrier in time, it could lead to loads of problems, including no coverage
- Concerns about over reporting, are mostly overblown. Not every incident, but if you think you have a data breach, report it.

What You Need To Know - Payments

- Cyber insurance policies typically can cover costs in two ways
  - Reimbursement
  - Pay on behalf

- Pay on behalf
  - More common these days, and means that the insurance provider will make the payments directly
  - In most cases you have less control of the process, and cannot select your vendors
- Reimbursement
  - Only a few policies offer this setup at this point
  - Allows insured to pick vendors, pay and submit reimbursement request

What You Need To Know - Panels

- Insurance carries are trying to keep prices low when they have to respond to a claim
- They do this by working with vendors to get them approved on “panels”
  - Legal counsel
  - Security vendors / forensics
  - Notification, Monitoring, Public Relations, etc.
  - Proactive services
- This is a great thing because it makes insurance dollars stretch further
- It can be a huge concern, if you have preferred vendors and relationships that you want to work with in the event of a data breach

What You Need To Know – Risk Management

- Risk Management Services and “Breach Coach”
- Some carriers use their risk management portals as a way to triage incidents
- They may require that you submit your initial issues via a portal that is provided
- They may required that you select a “Breach Coach” and have an initial conversation about the potential issue first
  - Legal Privilege
- Make sure you know the process before you need to use it!

What You Need To Know – Quick Response

- With the rise of Cyber Insurance:
  - It is clear incident responders need to understand how this impacts them and their processes.
- Most response teams focus on quick actions to get incidents under control / resolved
- This still is generally the right approach, but the notification of claim needs to happen almost immediately at the same time.


black hat
USA 2019
AUGUST 3–8, 2019
MANDALAY BAY / LAS VEGAS
Actions
RiskBased
SECURITY
#BHUSA @BLACK HAT EVENTS

Recommended Actions

- Continue to invest in the appropriate security controls
  - We don’t want Morale Hazards
- Define a response plan in case of a data breach
- Understand your exposures, data types stored and amount (number of records)

Recommended Actions

- Determine if you have a Cyber Liability insurance policy at your organization (**You NEED to know!**)
- If not, discuss transferring a portion of risk in the form of Cyber Liability insurance with management
  - Determine/review the coverage that would be important to your organization
  - Determine amount of desired coverage
  - Obtain a Cyber Liability quote and review the policy carefully!
- If appropriate, integrate Cyber Liability into your risk management plan

Recommended Actions

- Effective security programs cost $$$
- Yet, can still be compromised
- Cyber Liability cheaper than most controls and provides serious financial coverage including security services
- While there are “gotchas”, there are legit policies out there
- If you are a CISO and you have a breach. What do you want to say?
  - Whoops? Sorry.
  - We have a partner and coverage. Lets file a claim.

- Clear need for all organizations to develop an incident response plan
- Develop the plan prior to having a need to use it!
- Incident / breach response partners have value:
  - Included with Cyber Insurance
  - Negotiated Rates – can be used if past limits as well
  - Carriers have handled a lot of breaches!

Jake Kounds
@jkounds
jake@riskbasedsecurity.com
www.riskbasedsecurity.com

Discussion!

Integration of Cyber Insurance Into A Risk Management Program