Cyber Maturity Best Practices:
Bringing It to Life
Today’s Presenters

Phil Kibler  
Manager  
AIG Cyber Risk Consulting

- Responsible for strategy, development and delivery of AIG’s proactive cyber services delivered by consultants and partners
- IBM for 35 years, security for the last 10 years; led the global cyber security practice at IBM for 4 years
- Joined AIG in 2016

Dan Wilson  
Cyber Risk Consultant  
AIG

- Subject matter expert on cyber risks and solutions, acting as a technical resource for AIG underwriters, brokers and clients
- Certified security consultant and certified CISO
- 15+ years of experience in IT security
- 10 years experience in cyber incident response

Steve Morrison  
Director  
KPMG Cyber Response Services

- Cyber investigator and frequent speaker with over 20 years of technical experience
- Expert witness and court-appointed neutral expert
- Former AIG Information Security Manager
- KPMG Director since 2009
- Certifications include ENCE, GCFA, GCIH, and GNFA
Agenda

- Incident response planning and practicing
- An example tabletop exercise
- Why is this important To include in my cyber strategy?
Incident Response Planning and Practicing
What is a CSIRP?

A Computer Security Incident Response Plan (CSIRP) is a documented, pre-approved plan that ensures a repeatable process for efficiently managing cyber security incidents.

A CSIRP should:

- Define an incident and severity levels
- Define the incident response team and designate an incident manager
- Define roles and responsibilities for key team members
- Define the incident response process
- List critical systems, data, and vendor contacts
- Include important notifications, regulations, etc.
- Include communications plans
- **MUST HAVE MANAGEMENT BUY IN**
What happens when there is no plan?

- Panic!
- Confusion!
- Damaged evidence
- Underestimate the level of compromise – and how long they have been compromised
- Miscalculate the amount of data being stolen or systems being misused
- Failure to meet regulatory standards leading to fines
- Increased reputational damage

Establishing an incident response plan and practicing it regularly can reduce costs resulting from a cyber incident by 13.5%.

I’ve put together my CSIRP…now what?

Practice…Practice…Practice

- Tabletop exercises are a discussion based program in a conference room setting.
- The goal of the exercise is to examine the CSIRP to identify strengths, weaknesses, and items in the plan that require change.
- Tabletop exercises should be scheduled at least annually.
- Anyone that has a defined role in the Incident Response Team should attend.
How do tabletop exercises typically work?

- The designated facilitator will introduce a cyber incident scenario by providing background story along with any assumptions.
- The incident response team will follow their incident response plan and through facilitated discussion decide:
  - What is the severity level?
  - Who will take point?
  - What actions to take and who owns them?
  - Any communications (internal/external)?
  - Any legal, compliance, or other implications?
- When appropriate, the facilitator provides additional details or “injection” points to add information and keep the scenario moving forward.
- When the exercise is concluded, the participants should discuss what worked well and what didn’t.
  - Lessons learned and any actions to be taken should be documented, assigned ownership, and tracked to completion.
To be successful, you must establish ground rules

1. Everyone needs to participate.
2. Follow your Incident Response Plan.
3. You may not have all the information you need; make the best decision you can with what you know.
4. No idea is a bad one.
5. There are no right or wrong answers.
7. **Don’t worry about whether the exercise is a possibility or not.**
8. Remember, the goal is to improve your security program.
9. Practice worst case scenarios...prepare for anything.
10. Have fun!
An Example Tabletop Exercise
Example Tabletop Exercise

Background Information

One of your employees calls the IT helpdesk to report unusual behavior on her computer. She reports that she received an email earlier in the day that appeared to be legitimate, with information and a link about how your company’s employees could help with Hurricane Harvey recovery efforts. She was originally from Houston and very interested in helping people in the area she grew up in. However, after clicking the link in the email, she received an error page. After several attempts, she realized she could no longer open many of the key reports and files she works with and they appear to be corrupt.

She also received the following message on her screen:

“Your files are encrypted. To recover your files, you will require a key file for which you must pay 1 bitcoin to receive. If payment is not received in 3 days, your files will be permanently deleted.”
A few hours later, the IT help desk reports that they have received calls from other employees that have reported seeing a similar message on their laptop screen and are no longer able to work or access their files.

IT and IT Security are now involved and initial investigation shows the ransomware has spread to multiple end points and servers and is continuing to spread at a rapid pace.

There is concern that the ransomware may continue to spread and infect all systems.
Scenario # 1

Inject #2

- Unfortunately, it is now too late. All company systems, including systems managing your manufacturing lines are now encrypted and showing the screen demanding ransom payment for the decryption key.

- Your manufacturing lines are completely down, your online commerce site is down, and your company is now losing revenue by the minute.

- The ransomware variant has no available decryption key from any security vendor and, unfortunately, the ransomware made it to your connected backup service and all backups are also compromised.

- The CFO has received an additional email from an unknown source demanding 100 bitcoins in payment for the decryption key and to recover your data and systems. If the ransom is not paid in 24 hours, the email claims that a number of files will be deleted every hour thereafter until the ransom is paid.
Scenario # 1
Post Incident Debrief

- What went well?

- What didn’t go so well?

- What changes, if any, should be made to the Incident Response process as a result of this exercise?

- Other changes, if any, required to respond to this type of an incident?
Why is this Important to Include in My Cyber Strategy?
Why is this important to my organization?

- Tabletop exercises help an organization to:
  - Test their incident response plan and make changes where needed
  - Ensure a working repeatable process for different types of security incidents
  - Train team members on their roles and responsibilities within the plan
  - Increase general security awareness
  - Practice response to different types of incidents and prepare for new threats

- This results in:
  - A more efficient response to a number of security incident types
  - Less confusion and misunderstanding in the organization when incidents occur
  - An incident response team that is well trained and understands their roles
  - Less costs when the inevitable incident occurs

“Plan for what it is difficult, while it is easy.”

1Sun Tzu, The Art of War
Common missteps we often see:

- Individual roles are not clearly defined.
- The IR plan is too complex or too specific.
- No clear authority or chain of command.
- No severity classification for incident types.
- Poor communication.
- Overload key personnel.
- Plan is not practiced and/or key players not trained.
How can AIG help?

AIG’s Incident Simulation Workshop can help your organization practice and improve your incident response plan.

Preparation
2 weeks prior to workshop

Workshop
½ day workshop

Improvement
5-10 business days after workshop
KPMG Cyber: how can we help?

Keep It Simple – the Right Balance of Information Protection and Accessibility

PREVENT

Helping clients understand how best to align their cyber agenda with their dynamic business and compliance priorities.

IMPROVE

Helping clients build and improve their programs and processes, supported by the right organization and technology, to improve their cyber agenda.

DETECT

Helping clients maintain their cyber agenda as their business and technology programs evolve by providing greater visibility and understanding of changing risks.

RESPOND

Helping clients effectively and efficiently respond to cyber Incidents and conduct forensic analysis and detailed investigations.

Aligned with client business priorities and compliance needs

STRATEGY AND GOVERNANCE

PRE BREACH

TRANSFORMATION

POST BREACH

CYBER DEFENSE

CYBER RESPONSE SERVICES
Take aways

- Have a plan
- Practice your plan
- Ask what if….?
- The team that goes to the world series has played approximately 170 games to get there. Don’t show up on game day without ever having played or practiced before.
Questions?

Thank you for your participation!

Phil Kibler
philip.kibler@aig.com
317.967.3927

Dan Wilson
daniel.wilson@aig.com
303.514-3838

Steve Morrison
sjmorrison@kpmg.com
415.963.5486
American International Group, Inc. (AIG) is a leading international insurance organization serving customers in more than 130 countries and jurisdictions. AIG companies serve commercial, institutional, and individual customers through one of the most extensive worldwide property-casualty networks of any insurer. In addition, AIG companies are leading providers of life insurance and retirement services in the United States. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIGInsurance | LinkedIn: http://www.linkedin.com/company/aig

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries, and coverage is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds.

The data contained in this presentation are for general informational purposes only. The advice of a professional insurance broker and counsel should always be obtained before purchasing any insurance product or service. The information contained herein has been compiled from sources believed to be reliable. No warranty, guarantee, or representation, either expressed or implied, is made as to the correctness or sufficiency of any representation contained herein.

© American International Group, Inc. All rights reserved.