Incident Response

Will You be Prepared to Respond to a Cyber Event?

WEBINAR

{B(W)} CYBER SERVICES

Alaric COMPLIANCE SERVICES

PRESENTERS

MICHAEL BRICE

FOUNDER OF BW CYBER SERVICES

28 years of experience providing technology, security, and related cybersecurity consulting solutions for multiple industries, including deep commercial and military experience in the financial services industry as well as classified government operations. Received specialized training by the National Security Agency in Signals Intelligence. Former Marine Officer – served in the 1st Gulf War.

JOSEPH M. DIBARTOLO

DIRECTOR AT ALARIC COMPLIANCE SERVICES

Over 30 years of experience in the management and execution of compliance activities for SEC registered and unregistered investment adviser firms and private investment funds. He has served as an outsourced chief compliance officer to multiple SEC registered investment advisers. He has also executed several compliance consulting initiatives including SEC registration, compliance program design and risk assessment engagements with an emphasis on Alaric's hedge funds and private equity clients.

CYBER INCIDENT RESPONSE & INCIDENT RESPONSE PLANNING

- What is an Incident and what is an Incident Response Plan (IRP)
- SEC/NFA/FINRA Compliance Requirements per Incident Response
- What an Incident Response Plan should include
- How to stress-test your IRP
- How to determine who is qualified to lead your IRP

Increased Cyber Attacks are another "new normal" in the age of Corona remote operations

CURRENT SITUATION FOR THE “NEW NORMAL”

Rush to Remote Ops

IT Departments are told to do “whatever it takes” to get people connected from home…

Chaos, distraction, and conflicting business processes

Kids, investors, markets, capital calls, margin calls, redemptions and wires, wires, wires…

Then comes “The Incident”

Ransomware, E-mail Hack or Network Breach – usually with the intent to monetize (e.g., Bitcoin ransom or effect Fraudulent Wire)

WHAT IS A CYBER INCIDENT?

Per the Dept of Homeland Security: **An incident** is the act of violating an explicit or implied security policy according to NIST Special Publication 800-61. Of course, this definition relies on the existence of a security policy that, while generally understood, varies among organizations. These include but are not limited to:

- attempts (either failed or successful) to gain unauthorized access to a system or its data
- unwanted disruption or denial of service
- the unauthorized use of a system for the processing or storage of data
- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

Ransomware E-Mail Hack Network Compromise Webpage or System Disruption

In non-technical terms – it's when you have "Bad Juju of a malicious nature with your IT"

CYBER SECURITY IN THE NEWS – WEEK OF APRIL 20, 2020

- AST – Employee payroll breach
- San Francisco International Airport – Malware attack
- The Law Society of Manitoba – Ransomware
- Travelex – Ransomware
- Holland America – Accidental data sharing
- DESMI – Ransomware
- Ingram – Unauthorized account access
- Wappalyzer – Unsecured database
- Zoom – Thousands of Zoom credentials for sale on the Dark Web

WHAT IS AN INCIDENT RESPONSE PLAN?

Technically:

"An incident response plan is a systematic and documented method of approaching and managing situations resulting from IT security incidents or breaches. It is used in enterprise IT environments and facilities to identify, respond, limit and counteract security incidents as they occur."

Stated in "non-technical terms":

It's a document that helps your organization to quickly respond to cyber events in a structured, disciplined manner with the involvement of all key stakeholders (many of whom are not IT or security professionals) to minimize damage, maintain evidence and return to normal operations as soon as possible.

LET'S TALK OPERATIONS, NOT TECH…

In the asset management industry, an Incident Response Plan needs to be a combination of three key factors:

- Compliant
- Industry Acceptable
- Pragmatic

Without an Incident plan to incorporate these key factors, the following is destined to happen if you have a cyber Incident:

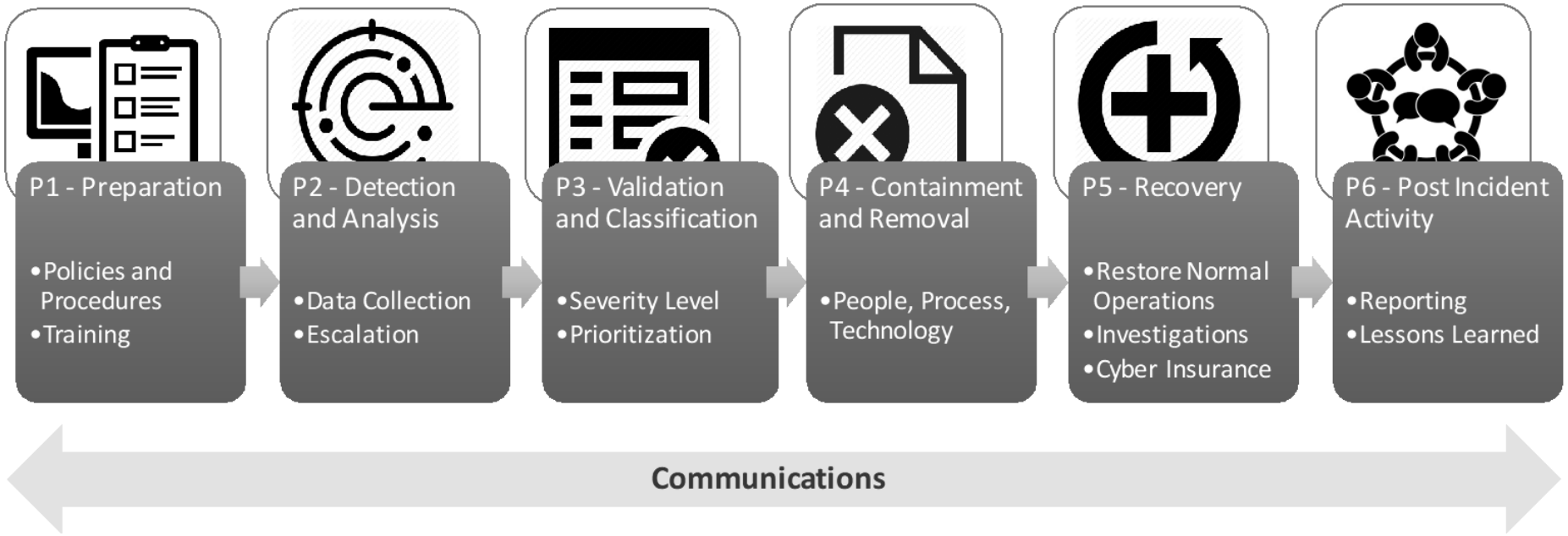
Time is lost, evident lost, improper fixes put in place, attacker alerted, regulatory issue, legal issues, privacy issues reputational impact, etc.

COMPLIANCE EXPECTATIONS

- SEC OCIE
  - Development of Incident Response Plan
  - Addressing Applicable Reporting Requirements
  - Assigning Staff to Execute Specific Areas of the Plan
  - Testing and Assessing the Current Plan

- NFA
  - Members must develop and implement information security plan (ISSP)
    - IR Plan is critical component of ISSP
  - Members must create procedures to notify NFA of a cyber-incident
- FINRA
  - Members expected to have an IRP for “most common attacks”

“INDUSTRY ACCEPTABLE” INCIDENT RESPONSE PLAN



Throughout each phase, the plan should address key questions such as:

What to do right now, whom to notify, when to coordinate, what info to capture, how to communicate, what to tell clients, who to notify legally, what to tell the regulators, what evidence to collect, what NOT to do…

Each phase should contain detailed checklists that map to specific Incident Use Cases (e.g., Ransomware, etc.)

“PRAGMATIC” INCIDENT RESPONSE PLAN

- Do you actually have an IRP?
- Is your IRP an industry acceptable plan based on key phases or a ‘paper tiger?’
- Does your IRP have checklists that map to specific Use Cases?
- Have the stress-tested it?
- Do you have an experienced security expert to lead it?

OUCH – WHERE TO START?

- Compliance and cybersecurity expertise need to be integrated
- Stress testing is critical – tabletop exercise with executive involvement is critical
  - Executives,
  - IT Leadership
  - Legal
  - Insurance Expert,
  - PR
  - Cyber/Forensics

And then there are the legal and regulatory issues associated with Personally Identifiable Information (PII)…

THE BOTTOM LINE

- Unfortunately, it's not a matter of “If” but “When” an organization is going to be attacked and suffer a cyber Incident
- Incident Response Planning is critical if you are the victim of a cyber Incident and especially if you have a data breach
- An Incident Response Plan is equally as critical from a regulatory perspective
- If you haven’t tested your plan and don’t have an Incident Response expert available to lead your plan, you most likely will learn that your plan was worthless

QUESTIONS?

THANK YOU

www.bwcyberservices.com
646-779-8976

{B(W)} CYBER SERVICES

www.alariccomplliance.com
888-243-2248

Alaric
COMPLIANCE SERVICES