CHART EXCHANGE

Coverholders And Risk Takers Exchange

Volume 4 • Issue 11
November 2019

Bridging The Gap Between Lloyd's of London And The U.S. Domestic Market

BEST-LAID PLANS...

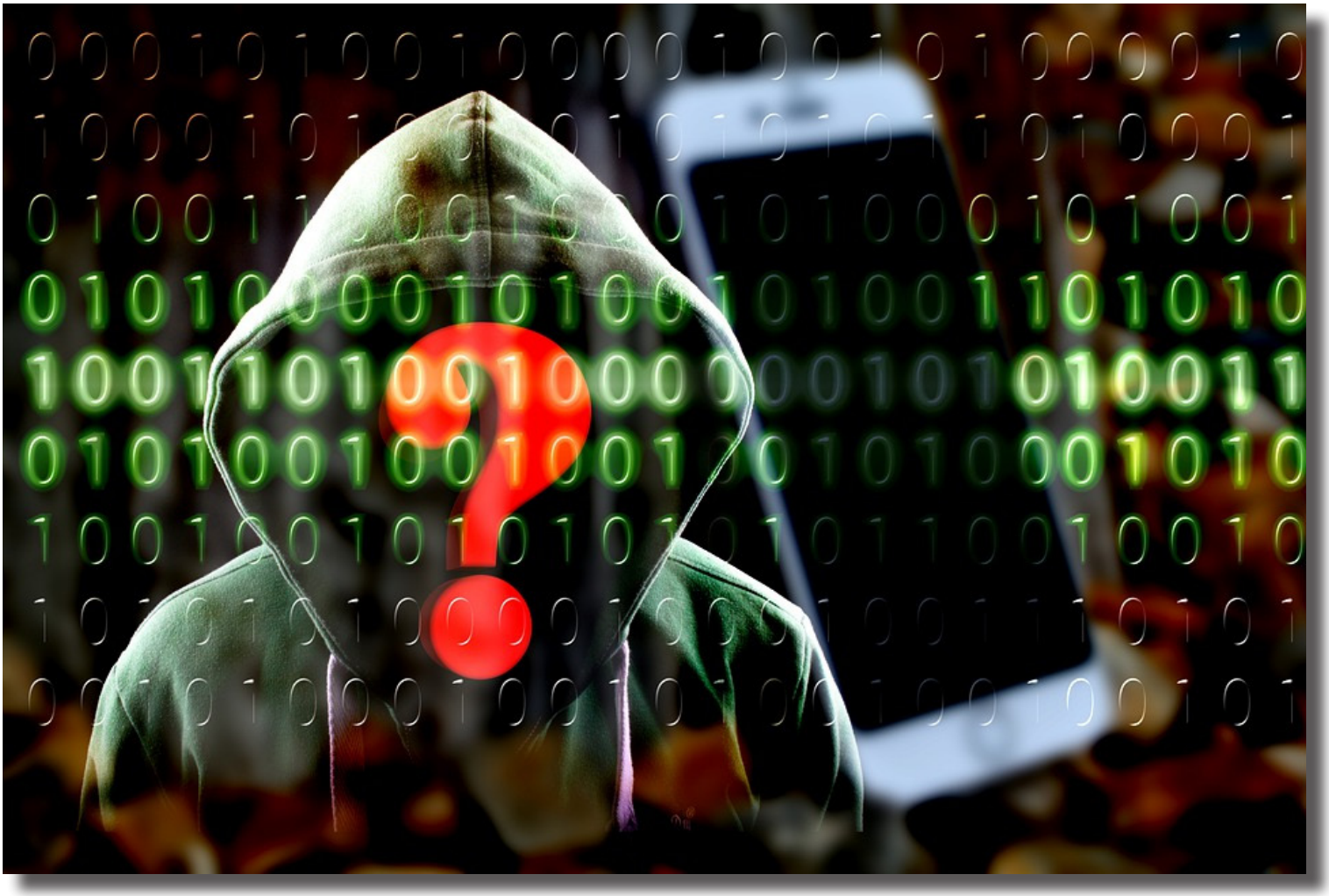
By Austin Berglas and Jennifer Rothstein

The famous quote from John Steinbeck's novella, "Of Mice and Men", is adapted from Robert Burns, "To a Mouse" poem; "the best laid schemes o' mice an' men…often go awry". This quote doesn't apply to cyber security planning. Studies have shown that a proactive approach to cybersecurity greatly reduces the chances of business interruption when an incident turns into a breach. It is high time for organizations of all sizes to take a proactive, defensive stance when it comes to cybersecurity. You must plan as if you have already been compromised, take a threat actor's view into your organization, and prepare for the inevitability that you will be targeted and breached.

A threat actor's view into your organization – while a bit unsettling – should help you assess:

- Have you performed any assessments to determine your risk level?
- Are you accurately measuring your cyber risk?
- Are your personnel properly trained to defend and respond?
- Do they understand what's expected of them to prepare and/or remediate incidents?
- As a leader, are you prioritizing

See Best-Laid Plans Page 32



Continued From Page 16

THE BEST LAID PLANS...

your cybersecurity roadmap to address risks appropriately?

Adversaries are going to get through your layered defenses eventually. No matter how high you build your walls, they will eventually get over them, but there are steps you can take to make yourself less attractive to threat actors. You don't want to be a quick and easy target. You need to secure your enterprise.

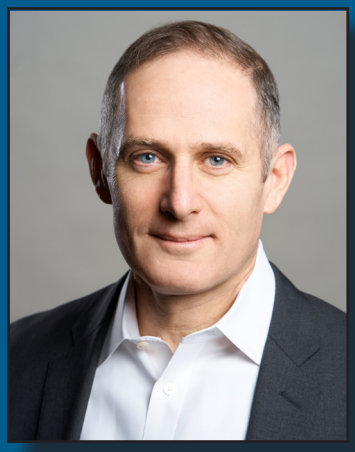
Planning is a crucial cybersecurity activity - the question of whether or not you'll be a target isn't a question at all. It's not "if" you'll be targeted, it's "when". Incident response planning allows you to develop both a strategic and a tactical plan for an incident. Your plan must include an examination of organizational information and security policies, and should be aligned with the organization's objectives.

When it comes to policies, your plan should outline in detail how your organization will respond to incidents. Once you have a plan, then you can begin to develop playbooks for specific incidents. Playbooks work like an "if/then" flowchart. For example, a ransomware playbook could include "If we are hit with WannaCry, then we will do 1, 2, 3, etc.". Playbooks can help you plan for fraud incidents, insider threats, and more. Each playbook should include actual step by step details about how the organization needs to respond to those particular incidents.

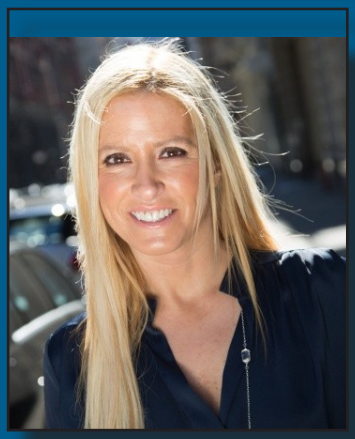
A proper plan will outline how you plan to accomplish and perform necessary tasks, such as a network isolation or host containment. Planning for a variety of scenarios will arm your organization with the actual step-by-step process necessary to make the proper decision under pressure. When the heat is on, you want to have a plan instead of panic.

Robust IR Plans will take into account the multiple business divisions, such as finance, legal, and HR. For example, when an incident strikes, the plan should ensure that the chief financial officer, the general counsel, the head of HR, and all personnel are aligned and coordinated so nothing is left up to chance. Don't simply talk about the "what ifs" and the responsibilities. Use a written plan that's been tested through a tabletop exercise so that everyone knows their role and responsibility.

As you build out your IR Plan, there are several key components to consider: a threat classification system, internal and external roles and responsibilities, processes for responding to incidents, and internal communications.
Classifications and Severity Matrix: Understanding whether an incident has a low, medium, or high impact on business operations will determine the severity and response. Using a matrix can help you triage.



Co-Author Austin Be
of Professional Servi
practice at K2 Intellig
years in the U.S. Gov
Agent in charge of th
oversaw all national
agency's largest cyb
Award for Excellence
achieved the rank of



Co-Author: Jennifer R
Insurance & Legal, for
in New York City. She
Women in Cyber Leade
rooted in STEM and th
for women to start and
efforts to providing eve
confidence to succeed
as Kroll and AIG, she h
with her deep knowled
demystify two complex
both cybersecurity and

- Low level: minimal impact, minor loss of operational efficiency
- Medium level: data at risk of exfiltration and may have been compromised, operations impacted
- High level: service disruptions, sensitive information exfiltration, data compromise

Levels should be assigned once you understand what has been impacted - from the asset type to the scale and scope of the threat.

Cyber insurers can help you prepare. Insurers are offering proactive services to encourage organizations to develop these plans. In addition to incident response panels, insurers are building proactive panels. This model allows insureds to access experts who can help with the pre-breach preparation. In fact, some insurers offer financial incentives to increase the uptake. The benefits are tangible; insurers position its insureds as better risks and in turn, they may reduce losses and claim payouts.

Further, the matrix outlined above mirrors the underwriters' criteria they factor into the risk evaluation process. Underwriters consider the impact an event will have on business operations and try to predict the possible frequency and severity of particular events – especially the current persistent threat of ransomware attacks.

It is imperative for you to take an analytical approach and an honest assessment of whether or not your current cybersecurity meets industry standards. Using tests and controls, you can ensure that your organization is more fully prepared, with policies and processes, to efficiently and quickly respond to a breach.

erglas comes to BlueVoyant as the Global Head ices after building and leading the Cyber Defense gence. Prior to K2 Intelligence, he served 22 vernment. Austin was the Assistant Special he FBI's New York Office Cyber Branch. There, he security and criminal cyber investigations in the er branch and was awarded the FBI Director's e in a Cyber Investigation. Prior to the FBI, Austin captain in the U.S. Army.

Rothstein is the Business Development Head, BlueVoyant, a cybersecurity provider headquartered also co-founded and serves as the President of ership Corp. As the cyber security industry has been e military, she recognized that it can be intimidating thrive within the space, and has dedicated her eryone with the tools, opportunity, knowledge and in cyber. Throughout her career at companies such as lead the effort in combining cyber expertise ge in insurance. She is driven by a resolve to x categories allowing access and understanding to d insurance in our increasingly interdisciplinary and

BlueVoyant

www.bluevoyant.com

- For insureds that need forensics, incident response, or proactive security services
- BlueVoyant is a pure play cybersecurity firm
- **WE GET IT** – we do it faster and better

Austin Berglas | Global Head of Professional Services
austin.berglas@bluevoyant.com

Vincent D'Agostino | Head of Cyber Forensics & Incident Response
vincent.dagostino@bluevoyant.com

Jennifer Rothstein | Business Development Head, Insurance & Legal
jennifer.rothstein@bluevoyant.com

Breached: incident@bluevoyant.com | **Info:** contact@bluevoyant.com