



REVELATIONS, REGULATIONS, & RISKS

CYBER EXPERTS WEIGH IN

Part Four: Emerging Threats





CLAY BLANKENSHIP

HEAD OF U.S. DIGITAL FORENSICS & INCIDENT RESPONSE
BOOZ ALLEN HAMILTON

[BOOZ ALLEN HAMILTON](#)



John Clay Blankenship (Clay) is a Principal Director at Booz Allen Hamilton. He heads the U.S. Incident Response Solutions team. Clay is a seasoned leader and a skilled digital forensic incident response analyst. Clay is a 20+ year law enforcement veteran with 18 years of experience in digital forensics, incident response, and high-tech criminal investigations.

2005 Clay initiated a cybercrime division for the Spotsylvania County Sheriff's Office in Virginia. During his time with the cybercrime unit, Clay obtained multiple industry certifications in digital forensics. He was certified as an expert witness in the Spotsylvania County Circuit Court and surrounding jurisdictions. Clay became an authorized trainer and coach for the International Association of Computer Investigative Specialists (IACIS). As a trainer, he has instructed digital forensic classes in the United States and Germany. Clay's post-law enforcement experience includes six years as an incident response analyst and engagement lead at IBM.

Before joining Booz Allen as part of the Tracepoint LLC acquisition, Clay was a Managing Director of Digital Forensics and Incident Response at Ankura. Clay was a member of Navigant's disputes, forensics & legal technology (DFLT) segment, which was acquired by Ankura in 2018. He has led several large and small incident response and forensic investigations for clients in many industries.

“

HACKER GROUPS ARE PORTRAYED AS THESE VILLAINOUS FIGURES IN A DARK ROOM SURROUND BY MONITORS. THAT IS LIKELY NOT THE CASE. THREAT GROUPS ARE LIKE COMPANIES WITH THEIR OWN ORGANIZATIONAL STRUCTURE.

WE ASKED, CLAY ANSWERED

Q: WHAT ARE SOME TRENDS THAT YOU ARE SEEING IN YOUR INCIDENT RESPONSE WORK?

At the moment, there are a couple of interesting trends. We recently observed discord among the ransomware group known as Lockbit. This conflict made us believe that offshoots were imminent. We saw an emergence shortly thereafter of INC ransomware, that uses similar tactics and has a similar leak site.

We have also seen an increase in pressure tactics by threat actors in attempts to make a victim pay. These tactics include Distributed Denial of Service (DDoS) attacks or straight harassment via phone calls and email.



**Q: ARE THERE
BASE CONTROLS
THAT
CONSISTENTLY
COULD HAVE
PREVENTED
THESE
INCIDENTS FROM
HAPPENING?**

All the critical controls are important. We have seen case after case that failure to implement is the root cause. For example, we consistently see failing to update and patch firewalls allowed a threat actor access. We have also seen where failure to update end-of-life software, such as operating systems, have been the root cause.

Q: WHAT ARE SOME THINGS INSUREDS CAN DO THAT WILL HELP TO PREPARE FOR AN INCIDENT?


In my opinion, the most important thing for an insured to do in preparation is to have an updated incident response complete with roles, responsibilities, and contacts. The contacts should include internal responders, external vendors, insurance, and legal contacts. Ensure they have a hard copy of this plan because digital copies will become inaccessible in the event of a ransomware attack. The insured needs to understand where the critical data resides.

Make sure backups are protected. An example is the 3-2-1 rule. Another thing to prepare is training and practice. Train internal first responders in preservation and containment. Conduct tabletop exercises annually or bi-annually to test the response plan.



What is the 3-2-1 Rule?
[View it Here](#)





Q: WHAT ARE SOME THINGS THAT INSUREDS SHOULD NOT DO WHEN THEY SUSPECT AN INCIDENT HAS HAPPENED?

One thing that the insured should not do is destroy evidence. We often see clients who bring in their local IT providers and have them rebuild before any preservation can be done. In most cases this is more costly than a forensic investigation because now their entire client base needs to be notified.

Do not arbitrarily restore to the closest backup if it is available. We often see that the threat actors have been in the environment days to weeks ahead of time. This could mean that the client is restoring to an already compromised state.

Also, in the event of a ransomware attack, do not reach out to the threat actor before consulting counsel and a professional firm. The legal team can help them navigate the pros and cons in communicating with the threat actor. If the insured needs to make contact, a professional negotiator should handle that.

Q: WITH THE SEEMINGLY CONSTANT STREAM OF HEADLINES, IS THERE SOMETHING YOU WISH THE PUBLIC KNEW ABOUT CYBERSECURITY? IS THERE SOMETHING THE HEADLINES ARE GETTING WRONG?

Cybersecurity is not something you can just do once and leave alone. It is a constant cycle. A company needs to always be thinking about security. They need to be continuously updating their security posture.

I also think that hacker groups are portrayed as these villainous figures in a dark room surround by monitors. That is likely not the case. Threat groups are like companies. They have their own organizational structures and chains of commands, from help desk to manager, and have affiliate programs, like franchises. For threat actors, a compromise is run just like a legitimate engagement.



SEE OUR KEY TAKEAWAYS:



Collaboration is critical to mitigating cyber exposure. Evolving cyber risk requires companies to coordinate preventive measures companywide, utilize the best security controls, and work closely with trusted partners in the cyber security community.

The BRP Cyber Center of Excellence provides more than expertise in placing cyber insurance coverage. We offer a broad range of integrated solutions and services that provide value to our customers by limiting the potential financial and operational impacts of cyber incidents. We work closely with companies across every industry to identify their specific vulnerabilities, mitigate current cyber risks, and stay ahead of new risks emerging on the horizon.



CONTACT US TO HELP PROTECT YOU AND YOUR BUSINESS.



This document is intended for general information purposes only and should not be construed as advice or opinions on any specific facts or circumstances. The content of this document is made available on an "as is" basis, without warranty of any kind. Baldwin Risk Partners, LLC ("BRP"), its affiliates, and subsidiaries do not guarantee that this information is, or can be relied on for, compliance with any law or regulation, assurance against preventable losses, or freedom from legal liability. This publication is not intended to be legal, underwriting, or any other type of professional advice. BRP does not guarantee any particular outcome and makes no commitment to update any information herein or remove any items that are no longer accurate or complete. Furthermore, BRP does not assume any liability to any person or organization for loss or damage caused by or resulting from any reliance placed on that content. Persons requiring advice should always consult an independent adviser.

Baldwin Risk Partners, LLC offers insurance services through one or more of its insurance licensed entities, including but not limited to AHT Insurance. Each of the entities may be known by one or more of the logos displayed; all insurance commerce is only conducted through BRP insurance licensed entities. This material is not an offer to sell insurance.