License to Hack

Understanding Risk and Emerging Trends in Cybersecurity

Takeaways from Baird's Cyber Webinar

Our Discussion

Baird recently hosted a cyber webinar, License to Hack, where a group of industry experts debated and discussed developments in the current threat landscape in the government and commercial organizations.

The experts focused on topics shaping the cybersecurity ecosystem and implications for the future, including:

- The role of nation-state threat actors, including China, Iran, North Korea and Russia
- Evolving government strategies and regulations
- Opportunities for enterprises & the evolving CISO role

In the following pages, Baird shares our top five takeaways from the Cyber Webinar: A License to Hack – all of which provide actionable intelligence for leaders navigating cyber risk, no matter the industry.

Thank You to Our Cyber Industry Panelists

Dan Turner
Vice President
Global Governments and Critical Infrastructure
Forcepoint

Bryan Ware
Chief Executive Officer
LookingGlass

Erin Whitmore
Director of Thought Leadership
Aon Cyber Solutions

Caleb Barlow
Information Security Entrepreneur
and Independent Consultant

Key Takeaways

See the following pages for in-depth insights

1 Nation States 'Allowing' Cyber Criminality to Thrive

Key nation states – including China, Iran, North Korea and Russia – have very little incentive to stop state-sponsored cyber criminality and hacking, they are, in fact, bordering on 'encouraging' it.

2 The West's Quest for Regulation

The West is pressing for stricter cybersecurity regulations and policy.

3 The Changing Role of the CISO

As cyber risk mounts for enterprises, the role of the CISO is coming into focus – and may take cues from the CFO role.

4 Don't Underestimate Ransomware

Ransomware is not only increasing in frequency it is evolving into a material threat for nation-states and enterprises alike.

5 Be 'Relatively' Clean: Cyber Hygiene Still Key

Enterprises should continue to champion good cyber hygiene. Simple solutions can have a major impact.

KEY TAKEAWAY #1:

Nation States 'Allowing' Cyber Criminality to Thrive

A small group of primary nation-state actors – including China, Iran, North Korea and Russia – play a major role in the overall cyber landscape. These nations are among the most prolific in terms of cyber criminality and currently have no incentive to end state-sponsored cyber criminality or hacking initiatives. Oftentimes, the nation-state is actively harboring cyber criminals and these initiatives are funding the regime. Therefore, there is no near-term catalyst to stop these criminals from continuing to create cyber challenges for the public and private spheres.

Erin Whitmore shared an overview of major nation-state actors in the cybersecurity landscape. Though Iran is largely sanctioned, it has very robust cyber programs and highly capable hackers. North Korea uses cyber crime from both a criminal activity and nation-state-directed activity perspective, with a notable number of cryptocurrency heists as well as some ideological hacking. Meanwhile, China typically employs nation-state activity for espionage and data collection of personally identifying information and health information. Russia differs from other players in that the line between criminal activity and state-sponsored activity is complex, with the harboring of criminal actors.

> "None of these countries are incentivized to stop the criminal illicit funds – the hundreds of millions of dollars that come into their economy from cyber criminal activity – from occurring."
>
> **ERIN WHITMORE**

KEY TAKEAWAY #2:

The West's Quest for Regulation

Western nations are pushing for new, stricter cybersecurity policies and regulations. Current rules aren't particularly impactful and have not yet led to meaningful change. Western nations are beginning to push for an elevated level of attention on cyber regulation. For example, U.S. government cyber leaders recently called upon Congress to establish a new branch of the U.S. military devoted to cybersecurity.

Cybersecurity has been based on voluntary partnership coupled with light regulation to date. While some enterprises have voluntarily embraced best practices and measures, too many have not – a trend that is hindering positive security developments as the world becomes more digitally dependent by the day. Regulation is on the horizon, but it will be a challenge for enterprises and nations to get the penalty dimension right.

"I think regulators are starting to recognize that although we may be reluctant to put down, 'Thou shall do the following,' into a regulation because of the time it takes these things to pass, the reality is... there are existing laws in the books that will allow for these things to be regulated and for fines to be levied, even without defining the exact cybersecurity posture."

CALEB BARLOW

"What we have to admit based on the state of cyber insecurity is that voluntary regime hasn't worked."

BRYAN WARE

KEY TAKEAWAY #3:

The Changing Role of the CISO

As cyber criminal activity continues to grow in breadth, volume and value, the C-suite and boards must take greater accountability for their cyber risks. The growing number of vulnerable entry points on enterprise networks, coupled with ineffective cyber policies, can lead to potentially catastrophic consequences for businesses. The panelist group agreed the role of the CISO is poised to evolve in the coming years and may become more similar to the CFO role in terms of influence, oversight and accountability. We are already seeing CISOs play a key role on boards, oversee outside assessments and audits, and advocate for investment in security needs. It is also worth noting that the recent changes in regulations have also put new burdens on the Board of Directors to have a better understanding of cyber threats and cyber posture of their businesses. It is likely that next-gen CISOs will be included in these discussions in the near future.

> "Where the CISO focus is largely on the delivery of IT services, the CISO historically has focused on risk mitigation. But even that is starting to change in that we are starting to see is the role of the CISO is really starting to become one where governance is required. Think of this in a lot of ways like the role of the CFO (Chief Financial Officer)."

CALEB BARLOW

> "People within cybersecurity need to start thinking holistically... no longer can you say, 'I'm exempt, I'm exempt.' If you have any presence on the internet, if you have any presence online, if you have any infrastructure and network – which everybody does – you can be a victim."

ERIN WHITMORE

KEY TAKEAWAY #4:

Don't Underestimate Ransomware

The volume of ransomware is ever-increasing, and it now poses a material threat to nation-states and enterprises alike. Ransomware continues to expand relatively unimpeded by government or corporate actions. Software vulnerabilities present another fruitful opportunity. This backdrop has allowed ransomware to expand and flourish in not only cyber venues, but the physical world as well by hacking mission-critical infrastructure.

In order to slow ransomware's advances, meaningful consequences must be established and enforced. As Bryan Ware shared in our discussion, "The best consequences are when [ransomware actors] are unable to either receive money or walk around with any freedom."

> "The most notable event was the Colonial Pipelines ransomware incident that not only had a cybersecurity component to it, but it bled into the physical world... it impacted ultimately energy supply on the East Coast of the United States. I think those kinds of wake-up calls, both of who's being compromised by ransomware actors and the real-world impacts it can have, are leading to a more aggressive posture amongst many countries."
>
> **BRYAN WARE**

> "Most companies do not have a nation-state threat – but all companies have a ransomware threat."
>
> **DAN TURNER**

KEY TAKEAWAY #5:

Be 'Relatively' Clean: Cyber Hygiene Still Key

There isn't a one-size-fits-all approach to cybersecurity. Each company needs to understand its risk aperture and take the necessary steps to become more cyber resilient. Sound cyber hygiene remains key in the current environment. Familiar tools like threat hunts, vulnerability assessments, internal monitoring and phishing awareness programs can make an impact. Simplicity and streamlining can also make a major impact. Streamlined security stacks are efficient and less likely to have gaps in visibility and coverage.

"Part of what we really struggle with in a boardroom is everything we deal with is relatively formulaic... When you're in a cybersecurity incident, you're up against a human adversary. They can pivot, they can jog, and they're going to keep punching you in the face until you learn how to punch back."

CALEB BARLOW

"Simplicity is the friend of the defender. Complexity is the friend of the attacker."

DAN TURNER

Navigate the Cyber Landscape with an Experienced Partner

Baird's Cybersecurity & Infrastructure Software team has an extensive breadth of experience as investors in and advisors to the sector. Our sector expertise covers network security, threat intelligence, security operations, data security, managed services as well as networking solutions, data infrastructure, DevOps and outsourced IT services. Our middle-market focus and reputation for excellence in transaction execution enable our team to deliver a great outcome for your company.

Simon Pearson
spearson@rwbaird.com
+44-20-7667-8409

Matt Russell
mrussell@rwbaird.com
+1-617-426-5424

John Song
jsong@rwbaird.com
+1-703-394-1832

Chelsea Smith
cmsmith@rwbaird.com
+44-20-7667-8342

Jonathan Kirkland
jakirkland@rwbaird.com
+1-703-394-1867

Marine Dumoulin
mdumoulin@rwbaird.com
+44-20-7667-8363

BAIRD

MALTEGO
Owned by
MAXBURG & Private Shareholders
Sale to
Charlesbank

REDLattice
Received Growth Investment from
ae Industrial Partners

Audax Private Equity
Majority Investment in
FLASHPOINT

NOVETTA
A Portfolio Company of
CARLYLE
Sale to
accenture

MATRIX42
A Portfolio Company of
EMERAM CAPITAL PARTNERS
Sale to
CortenCapital

TEAM CYMRU
has received a Growth Investment from
Audax Private Equity

View all transactions at rwbaird.com/transactions.