TAG
Security Annual
2025
SPECIAL REPRINT EDITION

PROTECTING LEADERS FROM HARMFUL NARRATIVES

AN INTERVIEW WITH WASIM KHALED,
CEO AND COFOUNDER, BLACKBIRD.AI

10 STEPS TO ENHANCE EXECUTIVE PHYSICAL SECURITY

WHY NATION-STATES ARE VULNERABLE TO QUANTUM THREATS RIGHT NOW

THE STATES OF CYBERSECURITY

TAG DISTINGUISHED VENDOR

BLACKBIRD.AI

The need to reduce cyber risk has never been greater, and Blackbird.AI has demonstrated excellence in this regard. The TAG analysts have selected Blackbird.AI as a 2025 Distinguished Vendor, and such an award is based on merit. Enterprise teams using Blackbird.AI's platform will experience world-class risk reduction—and nothing is more important in enterprise security today.

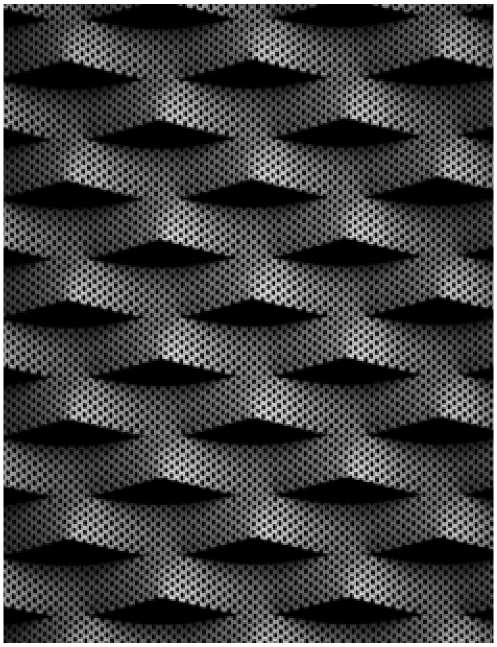
The Editors,
TAG Security Annual
www.tag-infosphere.com

REPRINTED FROM THE TAG SECURITY ANNUAL

AN INTERVIEW WITH WASIM KHALED, CEO AND COFOUNDER, BLACKBIRD.AI

PROTECTING LEADERS FROM HARMFUL NARRATIVES

In a world where AI-generated misinformation and coordinated disinformation campaigns can rapidly harm organizational reputations and financial stability, Blackbird.AI provides a cutting-edge solution. We recently spoke with Blackbird.AI to explore how their Constellation Narrative Intelligence Platform empowers organizations to detect, analyze, and mitigate narrative attacks. By combining AI-driven tools like Compass Context, Compass Vision, and Narrative Feed, Blackbird.AI equips executives with actionable intelligence to counter threats and maintain trust in an increasingly complex digital landscape.



TAG: How does Blackbird.AI's Constellation Platform empower executives to anticipate and mitigate the risks of harmful narratives targeting their organizations?

BLACKBIRD: Narrative attacks are a new threat vector targeting executives and organizations that cause financial and reputational harm. We created our Constellation Narrative Intelligence Platform to enable organizations to understand the harmful narratives caused by misinformation, disinformation, and deepfakes targeting their executives, organization, and industry, the influence behind them, the networks they infect, the anomalous–bot–behavior that scales them, and the cohorts and communities (threat actors, cybercriminals, nation states) that connect and amplify them. This has enabled our customers to make better strategic decisions with real data, especially during times of crisis, to reduce risk and financial and reputational harm to their organization.

The top narrative attack use cases we help organizations reduce risk and financial and reputation harm include Crisis events, executive protection, cyberattacks, brand protection, stock manipulation, financial market risk, mergers and acquisitions, breaches, geopolitical risk, physical risk, supply chain and critical infrastructure, environmental, labor relations, and insider threats.

TAG: How do the Compass Context and Compass Vision enhance narrative threat detection and decision-making for organizations facing complex, multilingual narrative attacks?

BLACKBIRD: Compass Context lets you gain context and clarity of any online claim, article link, or supported social media post or video. When you ask Compass Context a question or paste any link, it processes a query in real-time from thousands of sources, checks claims, analyzes results and generates an accurate, easy-to-understand answer with footnotes and citation links from trusted sources.

Compass Vision enables deep fake image and video detection, providing a clear 'AI-Generated' or 'Not AI-Generated' assessment score. With the increasing availability of AI tools in the hands of threat actors to create better and better deepfake images and videos, the challenge of recognizing what has been manipulated will only increase. Even more important is when a deepfake becomes a harmful narrative, the risk to the executive and the company increases exponentially.

Compass Vision enables deep fake image and video detection, providing a clear 'AI-Generated' or 'Not AI-Generated' assessment score.

When Constellation, Compass Context, and Compass Vision are combined. It allows organizations to identify misinformation, disinformation deepfakes, and the harmful narratives that sprout from them so that they can take action to reduce executive and company risk significantly.

TAG: How does Blackbird.AI's Narrative Feed enable C-suite leaders to stay informed about emerging risks and respond proactively to potential reputational or financial harm?

BLACKBIRD: Narrative Feed leverages our AI-based technology to quickly summarize and prioritize real-time risks and threats about emerging harmful narratives. It leverages the trillions of online engagements our Constellation Platform analyzes each month, providing concise, actionable intelligence in a summarized form that is easy for executives to understand and take action on.

TAG: With rising executive security concerns, how does Blackbird.AI help organizations analyze and neutralize coordinated online campaigns that might endanger individual leaders or corporate brands?

BLACKBIRD: Blackbird.AI identifies narrative attacks that are targeting executives and corporate brands, who is behind them (Cybercriminals, nation-states, threat actors), the networks they infect, the anomalous–bot–behavior that scales them, and the cohorts and communities that connect and amplify them. Having visibility into these harmful narratives as they escalate enables organizations to reduce risk and protect their leaders and brands significantly.

Our RAV3N Narrative Intelligence Team is a diverse group of intelligence investigators who work with our customers to provide deeper insights into the most impactful narrative attacks. They have data science, national security, cybersecurity, journalism, OSINT, and communications backgrounds and are power users of the Blackbird.AI Constellation Platform and our custom toolkits.

They also offer deep investigations and reporting, advanced benchmarking, learning programs, and professional services to boost our customers' narrative defense strategy. Our platform and RAV3N Team service complement any cybersecurity and physical security teams protecting executives and the company's brand.

TAG: As we are now in 2025, what narrative attack trends are you seeing that executives should be aware of and prepare for?

BLACKBIRD: In 2025, every executive and organization that creates shareholder value will be a target and is at risk. AI-powered tools, hyper agenda-driven information campaigns, and generative content creation have made it easier than ever for threat actors, cybercriminals, and nation-states to target executives and organizations by manipulating public opinion on a massive scale.

Organizations face a new threat vector of risk from harmful narrative attacks that manipulate public perception, destabilize stock prices, and erode stakeholder trust within minutes. Synthetic media, deepfakes, and AI-generated narratives are being used to fabricate press releases, forge executive communications across text and video conferences, or stage false crises, leaving organizations with a significant blind spot and scrambling to respond in real time.

Threat intelligence providers do not offer protection from narrative attacks. Narrative intelligence fills a massive cybersecurity gap. That's why we created Blackbird.AI to help global organizations fight back.

10 STEPS TO ENHANCE EXECUTIVE PHYSICAL SECURITY

JOHN RASMUSSEN

The murder of UnitedHealthcare CEO Brian Thompson in December shook up executive suites and boardrooms across the nation. Many organizations took note of the lack of physical security afforded to Thompson as he entered a hotel to attend an investor conference. Where was the executive protection? Had there been a risk assessment completed to understand the nature of threats to this CEO?

As a CISO, I have been a member of safety teams working with internal physical security and sometimes external law enforcement to create safety plans. I was privy to many different scenarios that could impact security, both physical and digital. Threats vary based on the size of the company, geography, revenue, and products. The threat actors could be individuals from ideological groups, dissatisfied customers, unhappy investors, or criminal gangs. The best way to prepare is to establish a program to counter them.

SECURITY RECOMMENDATIONS

These 10 steps can help enhance security for the leadership team. Many of these seem like a "no-brainer," but even as obvious as they are, they can help give the company an edge against threats. Approaching them in order, they start with the fundamentals and move to specific activities and mitigation techniques.

1 There will be a certain point where risk rises for a company, usually in a period of growth, and the risk gets heavier. At this point the company should bring in a third-party expert to conduct a physical security risk assessment for your executive leadership team. There are many companies that provide services that can look at physical security and cybersecurity for executives or other members of the organization. A simple internet search for "executive protection services" will yield many results.

If you are doing your first assessment, you should focus on the highest value targets rather than doing a broad assessment that extends beyond the C-Suite. Prior to engaging, seek references for the security companies you're considering from businesses in your same business sector.

2 Create an executive protection program. Any company, large or small, should have one of these in place. An officer of the company should appoint an executive to lead this effort. Usually this responsibility would fall under the chief operating officer or general counsel. The VP of risk management could also manage this function, but will need authorization from senior leadership to start the program.

Whoever is in charge of creating the program would typically tap the leader of the company's public safety department, typically titled "chief" (as in "chief of police"), to manage it and build a team that includes subject matter experts with expertise in both physical and cybersecurity risks. This program would focus exclusively on executive security and would take a multi-disciplinary approach.

WHILE THREATS AND RISK LEVELS MAY RISE AND FALL, BEING AWARE OF THE DANGERS AND ESTABLISHING A PLAN TO DEAL WITH THEM SHOULD BE FRONT OF MIND WHEN IT COMES TO EXECUTIVE PROTECTION.

3 Companies should develop and implement clear physical security policies. As part of their overall governance, they should establish policies and procedures so personnel understand what needs to be in place. This program should be governed the way other risk management programs are run, such as cybersecurity committees, compliance committees, and risk management committees. Depending on the scope of the physical security program, the policies and governance could even be rolled into one of those existing programs.

Controls related to these policies should be implemented and tested on a regular basis. An example of these controls would be wearing your ID badge visibly at all times in the workplace. Policies should be introduced across the organization, and staff awareness should be built through communications channels and by training responsible employees to execute and enforce them consistently.

4 Work with your internal safety/security team. Organizational leadership—from operations, to legal, to cybersecurity—should build relationships with their in-house security team. Many organizations view this as a support service to protect their property or personnel, but this group has much more to offer. They are your best first option for defense and advice to adapt to threats. Often these teams employ former law enforcement officers who are highly experienced and can offer insight into any threat intelligence they receive from their network. As a bonus, your security team may feel better utilized and included as part of the organization's mission.

5 Emergent situations can pop up any time. Creating a "threat assessment team" to plan for these situations and create safety plans is a great way to adapt as threats arise. These teams should consist of security, IT security, counsel, risk management, and human resources, at a minimum. Some organizations may have additional resources, like licensed mental health professionals, that could provide additional insight. The threat assessment team should be implemented by the leader of the executive protection program and governed by the same policies and procedures.

6 Design physical safety contingency plans that can be utilized on short notice. Having prepared plans, like changing office locations, setting up security escorts, or providing alternate communications devices, can quickly de-escalate an emerging threat. These are typically coordinated by the internal public safety leadership collaborating with cybersecurity and risk management leaders. The plans may require confidentiality, so they should be developed by a small team.

7 Consider digital security as a threat vector and implement controls to limit the potential attack surface. The digital security and physical security teams should work together to evaluate threats from the digital realm that could cross over into the physical. The two teams must coordinate to correlate the threat information in order to create a more complete picture of the risk. Often these teams fail to work together to connect the dots, even though they are both reporting conduits for incident identification. This occurs based on the traditional roles of the teams, and the best way to address this gap is for the digital and physical security teams to take the initiative to build collaborative relationships.

8 Conduct threat briefings periodically with executives. The security office, or public safety department for your business, usually led by a senior level “chief” who is responsible for overseeing the physical security for the entire organization, should be providing quarterly updates to leadership regarding threats to employees and leaders. Emergent risks should not be ignored. A public safety office may receive real-time threat intelligence from law enforcement, and the cybersecurity team will receive real-time data on digital threats.

At a certain threshold the leadership team should be informed of the threat. But filtering out threats can be challenging. As the program develops, the security office should learn which threats are more relevant and improve its ability to focus on the ones with a higher likelihood of doing damage. If there are too many alerts, the executive leader may ignore the threat briefings. The correct level will need to be determined by the leadership team and the security team. They need to ensure that the leaders don’t experience alert fatigue and end up missing real threats.

If a leader is travelling, the security team should be included in planning sessions to provide insight into threats at the intended destination.

9 Coordinate threat communications. Ideally, using your company’s public safety department will be the easiest route for coordinating threat communications, both incoming and outgoing, as it mirrors what most individuals are currently used to.

A threat can come in over text, voice, email, or other channels. When threats are received, there should be a coordinated effort to share the information among teams so evidence can be confirmed, collected, and consulted. The public safety department will work with corporate communications to build awareness of threats to the larger corporate community and will also act discretely with Risk Management, Legal, and others to communicate specific targeted threats.

10 Where possible and practical, executive threat protection should extend to the leader’s home environment. Home locations should be assessed by physical security experts for the softness of the target, and additional security measures should be set up to protect the executive’s family and home. This assessment can be completed by the company’s internal corporate security team or by a consultant. This can be coordinated by your chief of public safety, who will be able to recommend a vendor to evaluate physical security risks.

FINAL THOUGHTS

Corporations may not feel there are imminent threats to their executive teams, but taking a proactive approach and documenting contingency plans for physical security is way better than being surprised if something does arise. Companies should think about their business goals and areas of operation. Travel to cities within the United States may be routine, but are there issues you may not be aware of, like protests or strikes, that could impede an executive’s travel? Going abroad can generate different types of risks, like a kidnapping, robbery, or a physical injury (did you purchase medical evacuation insurance?). While threats and risk levels may rise and fall, being aware of the dangers and establishing a plan to deal with them should be front of mind when it comes to executive protection.

WHY NATION-STATES ARE VULNERABLE TO QUANTUM THREATS RIGHT NOW

DR. EDWARD AMOROSO

We know organizations that have relied on encryption to protect sensitive information will soon be grappling with the implications of a post-quantum era, where today's encryption protocols could be rendered obsolete. The concern surrounding store-now-decrypt-later methods is particularly pressing for organizations dealing with adversaries such as nation-states.

Our concern at TAG is that the most capable nation-state actors are often decades ahead in cryptographic research and espionage. As a result, we must assume that they are already gathering encrypted data with the intention of decrypting it when quantum computers become sufficiently powerful. But perhaps we should fear that sufficiently strong quantum computers might already exist in the basements of these powerful organizations.

Most businesspeople and technologists have been told by organizations such as the National Institute of Standards and Technology (NIST) that the timeline to Y2Q (year to quantum), when quantum computers will be able to crack widely used encryption, is still many years away. But in this article, we try to make the reasonable case that Y2Q could be much closer than most organizations realize, especially if their adversaries are nation-states, like the ones that are home to the NSA and GCHQ.

THE STORE-NOW-DECRYPT-LATER THREAT

This concept is a strategy that hinges on the expectation that while today's encryption remains robust, it can be broken in the future when quantum computers reach a certain level of sophistication. Nation-states and advanced threat actors are believed to be intercepting and storing vast quantities of encrypted data, knowing that it is only a matter of time before they can break it.

Classical encryption algorithms, such as RSA and ECC (Elliptic Curve Cryptography), rely on the computational difficulty of problems like integer factorization and discrete logarithms. These problems are considered intractable for classical computers, but quantum computers can solve them exponentially faster using Shor's algorithm. This means that once sufficiently powerful quantum computers are operational, these encryption standards will be broken.

The presumed danger for organizations is that once their encrypted data is compromised, it may already be too late. Sensitive data, including state secrets, intellectual property, financial transactions, and personal information, can be accessed retroactively, leading to breaches. It's not just about future communications being compromised—it's about everything that has been encrypted up until now being cracked once quantum decryption becomes viable.

SENSITIVE DATA, INCLUDING STATE SECRETS, INTELLECTUAL PROPERTY, FINANCIAL TRANSACTIONS, AND PERSONAL INFORMATION, CAN BE ACCESSED RETROACTIVELY, LEADING TO BREACHES.

But this is the rub: Everyone assumes that nation-state actors are no farther along in their quantum research than every other research and development team in the world (e.g., IBM). Experience dictates that this could be wrong. Remember, for example, that James Ellis invented public key cryptography at GCHQ half a decade before Diffie and Hellman.

NATION-STATES ARE AHEAD: THE NSA AND GCHQ

In fact, our view is that by any reasonable historical analysis, intelligence agencies like the NSA and GCHQ have been significantly ahead of the public cryptographic community. From early advances in cryptographic analysis during World War II to their leadership in digital encryption, these agencies have often been at the forefront of both creating and breaking encryption technologies—and they attract and employ the best talent.

The NSA's involvement in cryptography is particularly significant. It is widely believed that the NSA has had access to cryptanalytic techniques and computational resources far beyond what is known publicly. For example, the declassification of Cold War-era ciphers showed that the U.S. intelligence community had broken encryption methods long before the public cryptographic community believed them to be insecure.

While no government has openly declared having a fully operational quantum computer, it is not unreasonable to suspect that research divisions within organizations like the NSA or GCHQ have quantum computing capabilities in development. Given the high stakes of cyber warfare and espionage, these agencies likely have substantial quantum cryptanalysis programs aimed at foreign adversaries and even private organizations.

From the perspective of TAG, we fully admit to our national and geographic bias toward viewing the NSA and GCHQ as benevolent organizations. (And yes, we know that many of our readers will disagree.) That said, we would point out that many nation-state actors should not be viewed as so benevolent, and this is where we are most concerned. Readers can fill in their country of choice, but it seems reasonable that adversary nations are working in this area.

NIST'S QUANTUM THREAT TIMELINE MAY BE TOO CONSERVATIVE

NIST has been at the forefront of preparing the cryptographic community for the quantum threat. In 2016, NIST began a process to evaluate and standardize post-quantum cryptography (PQC) algorithms that are resistant to quantum attacks. NIST's official timeline for when quantum computers will be able to break classical encryption has been estimated to be between 10 and 20 years from now.

This timeline is based on several assumptions about the pace of quantum computing development, the technical hurdles that must be overcome, and the scale of quantum computers needed to break classical encryption. However, several experts believe this estimate is outdated and fails to account for the accelerated pace of quantum research or the secrecy surrounding nation-state programs.

We believe that for organizations dealing with sensitive information, the quantum threat is already here. These organizations cannot afford to assume that Y2Q is decades away, particularly given the possibility that adversarial nations are further along in their quantum capabilities than public research suggests. If such nations already have quantum computers capable of breaking encryption protocols, then Y2Q is effectively now.

RAPID ADVANCES IN QUANTUM COMPUTING

As further evidence, consider that the field of quantum computing is advancing rapidly. In recent years, companies like IBM, Google, and Honeywell have made significant strides in developing more powerful and stable quantum processors. Google famously announced in 2019 that it had achieved "quantum supremacy," demonstrating that a quantum computer could solve a problem faster than the world's most powerful classical supercomputer.

Quantum hardware is also steadily improving, with qubit counts rising and error rates decreasing. Researchers are also developing new techniques for error correction, a major hurdle in quantum computing, which will allow quantum computers to scale more effectively. With these improvements, the gap between theoretical quantum cryptanalysis and practical deployment is closing faster than anticipated.

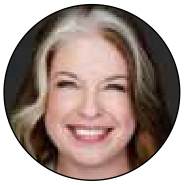
Several governments, including China's, have also invested heavily in quantum research. China's quantum efforts are of concern to the West, as the country has demonstrated leadership in quantum communication and quantum cryptography. Chinese research in quantum key distribution (QKD) and other aspects of quantum security suggests that the country is pursuing quantum dominance, which would have significant geopolitical implications.

PREPARING FOR THE QUANTUM THREAT

For organizations concerned with the quantum threat, the time to act is now. Waiting for public announcements of quantum breakthroughs could leave them vulnerable. Instead, organizations should begin transitioning to quantum-resistant cryptographic protocols as part of a broader post-quantum security strategy. NIST's ongoing work to standardize PQC algorithms provides a roadmap for this transition, but organizations must start preparing immediately.

Additionally, organizations should assess their long-term data protection needs. If encrypted data today is expected to retain its sensitivity for decades, then the risk of it being decrypted by future quantum computers is significant. By adopting quantum-resistant encryption methods today, organizations can mitigate the risk posed by store-now-decrypt-later strategies employed by adversaries.

THE STATES OF CYBERSECURITY



JOANNA BURKEY, SENIOR ANALYST, TAG

To get a real picture of the state of any given topic, it's common best practice to ask the experts. And there certainly are plenty of experts in cybersecurity to ask these days. In fact, just reference the other articles in this publication. But what about topics that are so far-reaching, so broad that they have a consistent and direct effect on an audience far larger than only experts? Cybersecurity is, without a doubt, one of these topics. It is difficult if not impossible to find anyone that is not in some way affected by this topic, so let's look at the state of cybersecurity from a few additional points of view.

We hear frequently that "perception is reality." And for three groups of people in particular, their perception of cybersecurity—and more importantly, their reactions in response—have a tangible and daily impact. These groups are: company employees, company officers and directors, and everyday citizens. The understanding of cybersecurity, and how understanding guides the actions of each of these groups, can have an outsize effect on the success or failure of cyberattacks that are in motion at any given time. So what is the prevailing zeitgeist amongst these particular populations? And is there a single one, or multiple, co-existing mindsets?

COMPANY EMPLOYEES

Let's start with the company employee, quite often and truly referred to as the most important company resource. It's certainly inarguable that the actions of an enterprise's individual employees are one of the most important factors on the scope and impact of a potential cybersecurity incident. Knowing this, CISOs for years have attempted to create a more "cyber savvy" workforce through a variety of tools: cybersecurity training, phishing tests, tabletop simulations (just to name a few).

IT IS OBVIOUS TO ALL THAT ALLOWING AN UNAUTHORIZED, BADGELESS INDIVIDUAL INTO A SECURE BUILDING IS A THREAT, BUT TRANSLATING THIS EQUIVALENT INTO THE DIGITAL WORLD IS EXTREMELY DIFFICULT FOR ANYONE WHO IS NOT A TECHNOLOGIST.

So why are we still in a place where most employees don't feel particularly empowered or educated? In fact, the emotion they express most often about cybersecurity is that it is "frustrating." Frustrating in all senses—either the employee has to contend with technology intended to make them safer, but that instead just gets in the way, or the employee is relied upon to make good cybersecurity decisions without having any particular cybersecurity expertise. This situation can also be frustrating for the CISO. If it's so straightforward for employees to understand that letting someone tailgate into a building is bad practice, then why isn't there the same intuitive understanding of the ills of password sharing?

Technology has moved so fast, and, driven by digital transformation, taken over so many of our ways of working, that we now have large numbers of company employees who understand how to use the technology but not actually how the technology works behind the scenes. It is obvious to all that allowing an unauthorized, badgeless individual into a secure building is a threat, but translating this equivalent into the digital world is extremely difficult for anyone who is not a technologist. As the pace of technology adoption, and the exponential curve of digital complexity increase, it is becoming more and more critical to consider the employee experience. Too often, technology is adding complexity and creating impediments to the employee function. This has an adverse effect not only on security but also on employee productivity overall.

OFFICERS AND DIRECTORS

Moving on to a smaller subset of the broader employee population, let's look at the C-suite and, by extension, the board of directors. The high-level strategic decisions made by company leaders have the potential to dramatically influence the cybersecurity posture of any given enterprise. This fact is well understood. For some years now it has been impossible to avoid discussing cybersecurity and its criticality in the boardroom and at the CEO level. What has been more elusive is how to translate that criticality into appropriate action and oversight.

Board directors and C-suite members are no strangers to risk discussions. It's not overly dramatic to say that risk discussions are literally the lifeblood of what the senior executives discuss and decide on every day. However, these risk discussions usually occur in a common, business-centric lexicon and relate to well-known topics such as the net present value (NPV) of a new project. Technology, and cybersecurity in particular, often bring their own jargon that can be difficult to put into analogous business terms. On the surface, the analogies between maintaining a fleet of company cars and maintaining a fleet of firewalls—software upgrades are like oil changes!—are obvious to practitioners but not obvious at all to business experts, who generally comprise the majority of board and C-level roles.

The outcome of this disconnect is the perception that cybersecurity is a new, strange animal when in reality it is business risk and opportunity in a different form. Without tech leaders and CISOs who can make that translation, the members of the C-suite and the board will continue to struggle to understand cybersecurity in relatable terms, impacting their ability to make optimum strategic decisions.

AVERAGE CITIZENS

Now broadening the aperture, do we see similar states of mind in everyday citizens? Just as there's a disconnect between the 3D world and the digital world for the everyday worker, and between "business as usual" and cybersecurity for senior executives, we see people across society grapple with how to identify cyber threats and avoid joining the line of global victims. A similar analogy to the office tailgating example comes to mind. It is easy to understand how locking a door protects the house, or how putting a seat belt on protects the passenger in a car. It is extremely challenging for most people to intuitively understand what the equivalents are in the digital world to these basic protections.

The state of mind this has engendered is one of confusion, fear, and helplessness. When so much of life is digital, as it today, the effects of a cyberattack can be fundamentally destabilizing, if not life-threatening. The ability of average citizens to conceptually understand the digital tools that surround them, and then use that understanding to guide appropriate action, is not at the level needed for a "cyber-savvy" society. This can manifest, at one end of the spectrum, in extreme avoidance and mistrust of the digital ecosystem; and at the other end, in a complete reliance on the producers of technology to protect their user base.

THE BOTTOM LINE

In conclusion, there is no single "state of cybersecurity"—unless we want to posit that the state is one of fragmentation, with more opacity than clarity. Each population discussed here struggles to make parallels between their world as they know it, and how to avoid and/or mitigate cybersecurity threats.

While cybersecurity experts define and implement enterprise strategies, ultimately the bottom-line impact of cybersecurity on the lives of everyday people depends as much on those same people as it does on the experts. The ability to make good choices while living and working in the digital world will continue to require better conceptual models for understanding—and an increased focus on developing frictionless guardrails in the digital medium.

BLACKBIRD.AI

Blackbird.AI protects organizations and executives from narrative attacks that cause financial and reputational harm. Our AI-driven Narrative Intelligence Platform identifies key narratives that impact your organization/industry, the influence behind them, the networks they touch, the bot behavior that scales them, and the cohorts and communities that connect them. This information enables organizations to make better strategic decisions to reduce risk, especially during times of crisis.
To learn more, visit Blackbird.AI.
For more information, visit Blackbird.AI.

TAG
DISTINGUISHED VENDOR

REPRINTED FROM THE TAG SECURITY ANNUAL