TAG

Security Annual

2025

SPECIAL REPRINT EDITION

FROM CHAOS TO CONTROL: MODERNIZING INCIDENT RESPONSE

AN INTERVIEW WITH MATT HARTLEY,
CO-FOUNDER & CPO, BREACHRX

PROTECTING THE U.S. BITCOIN RESERVE FROM CYBER THREATS

DIGITAL SAFETY AND PHYSICAL PROTECTION: BALANCING CONNECTION WITH CAUTION

WHAT IS A QUANTUM COMPUTER?

TAG
DISTINGUISHED VENDOR

BREACHRX

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

TAG 2025 DISTINGUISHED VENDOR

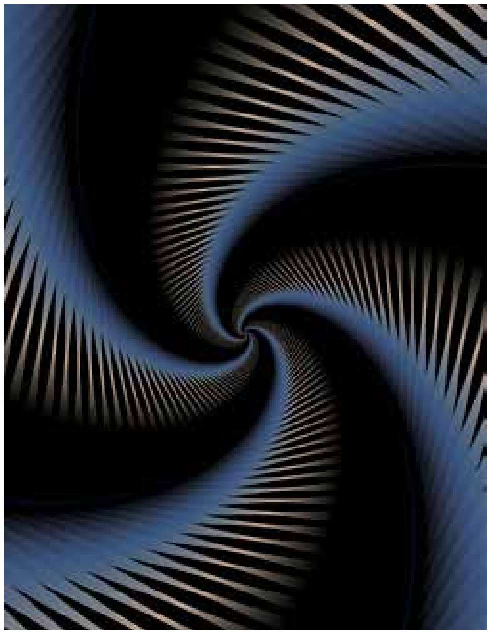
The Editors,
TAG Security Annual
www.tag-infosphere.com

REPRINTED FROM THE TAG SECURITY ANNUAL

AN INTERVIEW WITH MATT HARTLEY, CO-FOUNDER & CPO, BREACHRX

FROM CHAOS TO CONTROL: MODERNIZING INCIDENT RESPONSE

Today's landscape demands faster, smarter, and more collaborative response capabilities. BreachRx helps organizations meet this challenge by automating compliance, unifying workflows across legal, security, IT, and communications teams, and delivering real-time, actionable guidance—even in high-pressure scenarios. We recently sat down with BreachRx to explore how their platform redefines incident response in an era of rising regulatory pressure and evolving cyber threats. With the power of Rex AI, integrated exercises, and global regulation tracking, BreachRx transforms incident response from a manual, reactive process into a proactive, scalable operation.



TAG: How does BreachRx's incident response platform assist organizations in automating compliance with global cybersecurity and data privacy regulations?

BREACHRX: At BreachRx, our mission is to empower organizations to respond to incidents with confidence, clarity, and speed. Our platform unites all critical teams and business units in a single, secure environment, streamlining every phase of incident response from preparation to recovery. This facilitates cross-functional collaboration with strong communication, consistent metrics, and common goals.

When an incident occurs, BreachRx does the heavy lifting—automatically identifying relevant security tasks, regulations, and obligations, then assigning clear responsibilities across security, legal, privacy, and communications teams to ensure nothing falls through the cracks. Features like Rex AI and Cyber RegScout deliver real-time, plain-language guidance and actionable recommendations, helping teams act decisively, reduce manual effort, and avoid costly mistakes—while minimizing reliance on outside resources.

Centralized recordkeeping, audit trails, and automated reporting promote transparency, demonstrate compliance, and protect leadership from liability. By turning incident response into a proactive, scalable operation, BreachRx helps organizations move beyond reactive playbooks—ensuring resilience is about safeguarding the business, not just its technology.

TAG: With the introduction of Rex AI, how is BreachRx leveraging generative AI to enhance operational incident response capabilities?

BREACHRX: We've combined our unparalleled incident response dataset with generative AI to make response faster, more intuitive, and more reliable. Rex AI builds on BreachRx's incident response expertise and lifecycle-driven approach to deliver real-time, plain-language guidance tailored to each incident and business context. The goal is to eliminate guesswork and help teams act quickly and confidently—no matter how complex the incident or regulatory environment is.

Proactive preparation is key. Rex AI includes a conversational regulatory assistant, automated documentation, content revision, idea generation, and intelligent prompts that guide teams through every step. By automating time-consuming tasks like report drafting, legal research, and compliance tracking, Rex AI frees teams to focus on resolving incidents and protecting the business.

Rex AI builds on BreachRx's incident response expertise and lifecycle-driven approach to deliver real-time, plain-language guidance tailored to each incident and business context.

Ultimately, Rex AI is about making incident response smarter and more accessible. This represents a significant step forward in operational resilience within today's rapidly evolving cyber environment.

TAG: Can you elaborate on how BreachRx's platform facilitates integrated incident response exercises to prepare organizations for real-world cybersecurity incidents?

BREACHRX: Our platform is built to ensure organizations are truly prepared to handle cybersecurity incidents in a way that protects the business and its leadership from liability. What sets us apart is our ability to deliver next-generation incident response—not just digital forensics and containment but seamless incident management and communication.

BreachRX enables integrated, realistic exercises that unite security, legal, privacy, IT, and communications teams to rehearse incident response scenarios tailored to each organization's industry and regulatory environment. BreachRx dynamically guides participants through their specific operational, regulatory, contractual, and organizational obligations—ensuring everyone knows what's required before, during, and after an incident. Exercises can be run synchronously or asynchronously, allowing for more frequent training without disrupting day-to-day responsibilities.

By centralizing communication, documentation, and task management for exercises and live incidents, the platform creates a clear record of due diligence and coordinated response—crucial for proving compliance and managing legal or regulatory scrutiny. Continuous updates and actionable insights help organizations stay aligned, clarify roles, and reduce risk as threats and requirements evolve.

TAG: How does BreachRx help organizations meet stringent deadlines such as the six-hour notification requirement mandated by India's CERT-In directive?

BREACHRX: Meeting tight regulatory deadlines is a significant challenge for any organization. At BreachRx, we understand the pressure teams face when every minute counts. That's why we built our platform to simplify and accelerate the incident reporting process.

When an incident happens, our platform quickly analyzes the situation against our comprehensive, up-to-date regulatory library and instantly generates a clear, prioritized action plan, including what additional information needs to be gathered, given the situation. This means organizations no longer scramble to interpret complex rules under tight time constraints. Instead, they get straightforward guidance on what needs to be done, by whom, and exactly when.

We also enable teams to work seamlessly across security, legal, and compliance departments by assigning tasks and tracking real-time progress so nothing falls through the cracks. As tasks are accomplished, the action plan is updated automatically to reflect what's been discovered. Underpinning is our centralized reporting and a clear, detailed audit trail that organizations can rely on to keep leadership informed and demonstrate compliance during reviews or investigations.

Ultimately, BreachRx empowers organizations to meet demanding deadlines confidently and efficiently, reducing risk and helping maintain trust with regulators, customers, and partners—even in high-pressure situations.

TAG: What strategies does BreachRx recommend for organizations to proactively manage and respond to potential security incidents in areas critical to their business?

BREACHRX: We encourage organizations to take a proactive, business-wide approach to managing and responding to security incidents, especially in critical areas. The first step is moving beyond static, generic plans and adopting dynamic, actionable playbooks tailored to your unique risks, regulatory requirements, and business priorities. Our platform helps teams stay ready by automatically updating response plans as internal procedures, regulations, contracts, and other requirements evolve, so you're never caught off guard.

We also recommend regular cross-functional exercises to ensure everyone, from security and IT to legal, communications, and leadership, knows their role and can collaborate seamlessly when an incident occurs. By centralizing all incident response activities in one system, organizations gain clear visibility, defined responsibilities, and a secure real-time communication and documentation environment.

Finally, automation is key. BreachRx streamlines the entire response lifecycle, from identifying the right steps to assigning tasks and tracking progress, so your teams can focus on protecting what matters most instead of scrambling to interpret requirements under pressure. By making incident response routine, actionable, and integrated across the business, we help organizations minimize risk, recover faster, and reduce the cost of an incident.

PROTECTING THE U.S. BITCOIN RESERVE FROM CYBER THREATS

DR. EDWARD AMOROSO, SENIOR ANALYST, TAG

As you no doubt have heard, plans are in place to establish a Strategic Bitcoin Reserve and Digital Asset Stockpile, with the goal to position the U.S. as a leader in cryptocurrency. The reserve will presumably be funded with Bitcoin seized in criminal or civil asset forfeiture proceedings, ensuring no additional cost to taxpayers.

This overall initiative seeks to capitalize on Bitcoin's fixed supply and its potential as a unique store of value in the global financial system. An **executive order** dictated that as part of this initiative, federal agencies must provide a comprehensive accounting of their digital asset holdings to ensure proper oversight.

In addition to the Bitcoin reserve, the order established a stockpile to manage other digital assets obtained through forfeiture. The administration emphasizes that this move is part of a broader strategy to harness the power of digital assets for national prosperity. **David Sacks**, appointed as the White House's AI and crypto czar, likened the reserve to a "Digital Fort Knox."

This development marks a shift in U.S. policy, reflecting a recognition of the importance of cryptocurrencies and digital assets in our economy. Securing this stockpile and reserve, however, will require addressing security issues across multiple layers of infrastructure. This brief analysis presents our view first of the threats this development introduces, and then possible defenses that might help mitigate those threats.

SECURITY THREATS TO U.S. CRYPTO RESERVE

It is reasonable, before we propose our security plan, to first pore through the threats relevant to this new Bitcoin reserve. The bottom line regarding security is uncomfortable, but here it is: If hackers, criminals, or nation-states find a way to compromise or steal our national stockpile of crypto, it will be gone. Period. End of story.

Some readers might protest, suggesting that surely there would be a centralized means for establishing control, but the whole point of crypto is to avoid such control. Crypto is based on a decentralized peer-to-peer system that evades traditional oversight. With Bitcoin, you swap the security of regulatory oversight with the security of the software that holds your coins.

Let's tick through nine specific threats that should worry any practitioner tasked with tending to security for this stockpile. We should also remember: When you have any type of stockpile, you are just *screaming* to adversaries that you've placed a large number of eggs, so to speak, into one basket. Our reserve will be a target for every crypto hacker on the planet.

One more thing: We do not have decades of experience protecting crypto, so this is all new ground for most security teams. We can therefore be 100% certain that security errors, misconfigurations, and oversights will occur. I should say this again: Since this is a new area of security, we will see protection mistakes made—for sure.

THREAT 1: KEYS.

Let's begin with cryptographic keys. Our national stockpile will be protected by various public and private key pairs, which assumes that we would distribute the stockpile across accounts. Lose the private key for any wallet with crypto, and you are breached. Private key compromise through hacking, insider threats, or physical attacks is thus a major threat.

THREAT 2: HANDLING

The crypto in the stockpile will presumably be used for different purposes, including payments, withdrawals, and other operations. The problem is that any bugs or exploitable vulnerabilities in the smart contracts that govern these fund withdrawals and spending could lead to security issues—and again, this is not something that can be adjudicated in court.

THREAT 3: EXCHANGES

If reserves are held in or moved through crypto exchanges, which seems likely, then they become big targets for hacking and insider threats. Recognize that exchanges are built from software, including open-source, and they are thus prone to insider attacks, malware, and other types of exploits that we see so often across various industries.

THREAT 4: NATION STATES

State-sponsored hacking groups using zero-day exploits, social engineering, or supply chain attacks will most definitely use whatever means available to steal from our reserve. This is likely to include novel zero-day (0-Day) vulnerabilities discovered by elite offensive actors in countries such as Russia and China.

THREAT 5: INSIDERS

Rogue U.S. government employees or contractors, or ones who are vulnerable to coercion tactics (e.g., blackmail, bribery, extortion), will be major security challenges for the management of our stockpile. People will be required to manage this asset, and if a sufficient number go bad or collude, then we will lose our money.

THREAT 6: TRANSACTIONS

Attackers intercepting transactions or exploiting network vulnerabilities can create havoc for our national stockpile, and I am not sure that sufficient controls would be in place even to detect in real-time that this is happening. This is an area that demands more government-funded research, especially if we are going to stockpile crypto.

THREAT 7: MALWARE

Malware introduced via compromised software, firmware, or hardware is an obvious threat. In fact, this is one that perhaps resonates most clearly with practitioners. The supply chain for the systems, wallets, and other tools that will be used to manage and trade crypto will be tough to easily characterize (e.g. using a SBOM or similar).

THREAT 8: QUANTUM

Future advances in quantum computing breaking existing cryptographic security are an obvious concern. Remember that we are relying on public key cryptography to protect this pile of money. If some nation-state has quantum machines in their intelligence basement doing cryptanalysis, then they can break the anonymity of transactions.

THREAT 9: EXTORTION

Criminal groups targeting individuals with access to keys via ransomware or coercion will be a threat vector we can expect. That is, when someone gains access to one of our systems, we should expect that they will not only steal our currency but will probably also assign some sort of additional ransom or extortion demand.

PROPOSED NATIONAL PLAN TO PROTECT THE CRYPTO RESERVE

The list of threats outlined above should come as no surprise to anyone (like me) who has been tasked with protecting national infrastructure and resources at scale. Thus, I feel obliged and reasonably well-positioned to propose a series of protection strategies that our government had better engage before we see our stockpile disappear like smoke.

My approach is to describe controls that line up roughly with the vulnerabilities listed above. I will admit that this is a richer topic than I've been able to apportion time to review, so I'm 100% certain that I'm leaving some things out. But I hope whoever will be doing this work (and I have no idea who that will be) will benefit from this first pass.

CONTROL 1: CUSTODIAL AND WALLET SECURITY

A process must be put in place to ensure that the team engaged with protecting our stockpile is using multi-signature wallets that require multiple trusted parties to approve transactions. I know this sounds obvious, but it must be reinforced. I'd also recommend using hardware security modules (HSMs), air-gapped cold storage, and regular rotation and refresh of keys.

CONTROL 2: SMART CONTRACT AND PROTOCOL VULNERABILITIES

We should conduct regular security audits with third-party security firms to ensure avoidance of weaknesses in smart contract and other protocols. The money amounts will be large enough to perhaps even use formal verification methods to validate contract integrity. The goal should be time-locked transactions to delay withdrawals and enable security responses.

CONTROL 3: EXCHANGE AND TRADING SECURITY

I think it would be wise to leverage non-custodial storage to minimize reliance on exchanges. Whoever is in charge should employ whitelisted withdrawal addresses for fund movement. And, as with pretty much all of these controls, there should be continuous monitoring and review of exchange security posture.

CONTROL 4: NATION-STATE CYBER THREATS

I worry about nation-states, because it is naïve not to expect Russia, North Korea, and China to set their sights on this stockpile. Sadly, we might see Canada, Mexico, and (ahem) Greenland come after us as well. To that end, we'd better maintain separate and redundant security layers to minimize the threat (e.g., redundant cold storage).

CONTROL 5: INSIDER THREATS AND PHYSICAL SECURITY

This is a tough one, because compromised insiders are difficult to spot. Obviously, we must implement role-based access control (RBAC) and need-to-know access. I'd suggest use of multi-person authorization for transactions and key management. I guess we should also conduct background checks for personnel with access (even though DOGE has broken this habit).

CONTROL 6: INFRASTRUCTURE AND NETWORK SECURITY

This one involves the infrastructure. Someone should be ensuring that we are using private, permissioned blockchain nodes to manage the reserve. This should involve use of end-to-end encryption for blockchain transaction communications. All the usual network security measures should also apply (e.g., regular patching and hardening of Internet-facing systems).

CONTROL 7: SUPPLY CHAIN ATTACKS

The use of commercial vendors will be required (hint: preference will be given to U.S. firms), and I guess security assessments and audits should be used to reduce risk. I'd also recommend maintaining offline backups and forensic tools to detect tampering. As you would expect, we will also need to regularly refresh and verify wallet integrity.

CONTROL 8: QUANTUM COMPUTING THREATS

I know NIST is predicting several years of safety, but I suspect that nation-states are farther along in their use of quantum computers to cryptanalyze ciphertext than we think. To that end, we should transition to post-quantum cryptography (PQC) as it becomes available, perhaps using hybrid cryptographic approaches to ensure long-term resilience.

CONTROL 9: RANSOMWARE AND EXTORTION

I don't have a great solution here, but maybe by deploying air-gapped, geo-distributed cold storage we can avoid extortion. I think we can also implement self-destruct mechanisms for wallets under duress conditions, but I'm not sure how that would work. I would also train security personnel (whoever they are) on anti-extortion protocols.

CLOSING REMARKS

I have tried to identify likely hacking threats to the U.S. stockpile and reserve, and I hope my security plan helps the right person or group build a good defense. My fear is that this will not happen—and we will build the reserve with little security oversight. If this happens, then my prediction is that the balance will be hacked, and we'll be left with an empty U.S. wallet.

DIGITAL SAFETY AND PHYSICAL PROTECTION: BALANCING CONNECTION WITH CAUTION

DAVID NEUMAN, SENIOR ANALYST, TAG

The shocking murder of Brian Thompson, the CEO of UnitedHealthcare, has heightened awareness about the importance of physical protection, particularly for high-profile individuals. This tragedy offers an opportunity to consider how physical safety and digital awareness intersect. Our digital personas, shaped by the information we share online, from professional milestones to personal routines, are increasingly part of the safety equation.

Many questions remain about what happened in early December that allowed a shooter to wait unobserved along the precise path the CEO would walk on the way to a shareholder meeting he would never address. What we do know suggests that far from a random act of violence, the killer knew in advance where and when Thompson would arrive at the location where he was shot.

We know that Thompson's wife told NBC that her husband had received threats. This revelation prompts important considerations: Were these threats received digitally? And if so, did they alter his risk profile or security measures? Understanding the nature and delivery of these threats could reveal whether his digital presence played a role in his tragic death.

Additionally, the timing and location of the attack suggest that the assailant obtained detailed information about Thompson's plans and plotted his actions based on what he'd learned. The attacker was observed arriving outside the hotel just 10 minutes before Thompson, over 90 minutes before the scheduled start of the shareholder meeting. How did the assailant know that Thompson was not staying in the hotel where the meeting would be held, and how did he know precisely when the CEO would arrive?

These details underscore the necessity of evaluating physical and digital vulnerabilities when guarding the safety of high-profile individuals and all employees. The interconnected nature of today's world demands a comprehensive approach to personal protection, considering how those with malicious intent could exploit digital footprints and real-time information.

AN OFFLINE LIFE, AN ONLINE THREAT

It isn't only executives at large corporations who are at risk. These days, you don't even need to be digitally literate to be targeted by digital thieves. Years ago, as an executive director in EY's cybersecurity practice, I was asked to investigate a perplexing case involving a man in his 90s who had become the target of a criminal scheme. The man, a proud WWII veteran, had no online presence. He did not own a smartphone, nor did he use email or social media. Yet, criminals had identified him as a vulnerable target, calling him with a terrifying story: His grandson had been in a devastating car accident while traveling in Europe and urgently needed tens of thousands of dollars for life-saving surgery. Distraught, the man was on the verge of transferring the money when he hesitated just long enough for family members to intervene.

How did the criminals find him? The answer lay in his family's digital pride. Grandchildren had posted photos of him in his uniform, accompanied by heartfelt captions celebrating his service. They tagged their locations and shared moments of family gatherings, providing a rich tapestry of information. From those posts, the criminals pieced together enough to craft their exploit, targeting a man who, by all traditional measures, had no digital exposure.

WHEN DIGITAL NORMS BECOME A WAY OF LIFE

The information domain has fundamentally transformed the way we communicate and share. In the past, milestones, daily activities, and relationships were celebrated and shared within small, trusted circles. Today, social media platforms, professional networking sites, and even messaging apps have created a culture where sharing information about our lives feels almost compulsory—a digital norm that shapes how we present ourselves to the world.

However, corporate executives must approach these new norms with extreme caution, prioritizing their personal safety and the broader interests of their organizations. Oversharing personal details, locations, or daily activities not only increases the risk of physical harm, such as stalking or targeted violence, but it can also undermine an executive's professional credibility and the company's reputation.

For this reason, corporate governance over an executive's digital persona should not be optional. It is as critical as compliance with insider trading laws or maintaining a harassment-free workplace. Just as violations of those standards are considered serious, potentially fireable offenses, failing to adhere to governance protocols for digital behavior should carry similar weight. Establishing and enforcing clear policies for how executives manage their online presence ensures alignment with the organization's values, protects personal safety, and upholds the trust placed in leadership.

RISKS IN SHARING INFORMATION

These digital behaviors often feel harmless—positive, even. Sharing our lives online strengthens connections, celebrates achievements, and builds community. But when viewed through a risk lens, their implications become clear. The information we share can inadvertently create a roadmap for malicious actors to exploit vulnerabilities, in both the digital and physical realms.

Consider how patterns of behavior emerge from daily routines shared over time. A few social media posts about visits to the same coffee shop, gym, or lunch spot can reveal predictable movements to anyone paying attention. Real-time visibility presents another concern. Sharing updates while on vacation may seem like a great way to connect with friends, but it also announces an empty home, potentially making it a target for burglary.

Then there are personal connections. Posts about family milestones, relationships, or special moments can provide fodder for emotional manipulation or scams. This was evident in the case of the WWII veteran targeted through his grandchildren's posts, which offered enough information for criminals to craft a believable story.

Professional exposure can just as easily become a vulnerability. Announcing speaking engagements or travel plans publicly, while common in many industries, can provide opportunities for targeted attacks on individuals or events.

REEVALUATING DIGITAL NORMS THROUGH A RISK LENS

What advice can companies offer to enhance executives' own digital safety and that of their inner circles? Here are a few suggestions to help foster a culture of awareness, intentionality, and proactive decision-making.

Cultivating a Mindset of Awareness: Encourage executives and their families to understand the unique risks they face, focusing on how their digital behavior can impact safety and privacy. This mindset should guide all online actions.

Encouraging Open Dialogue: Promote continuous communication within the executive's inner circle about digital habits, privacy concerns, and the potential consequences of online actions. A collaborative approach ensures everyone feels informed and accountable.

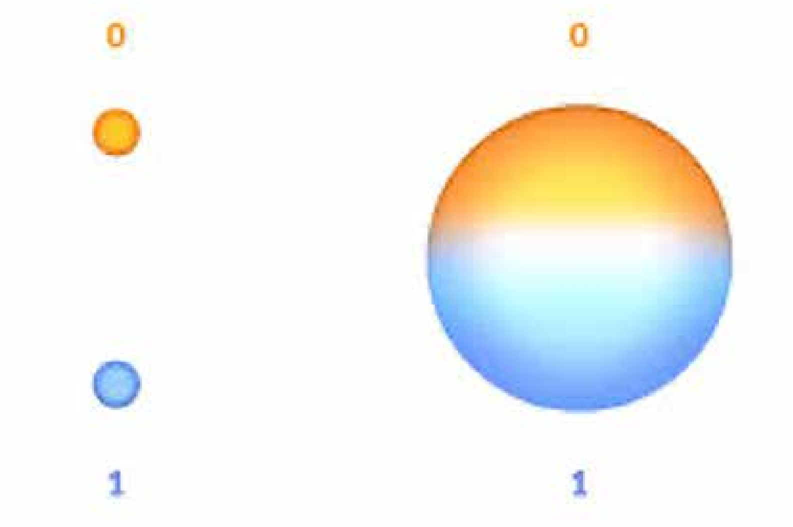
Focusing on Education: Invest in ongoing education for the executive and their family members about the evolving digital landscape, including emerging threats and safe online practices. This method avoids prescriptive tasks by building knowledge and confidence in navigating digital platforms safely.

Empowering Individual Responsibility: Instead of restrictive rules, focus on empowering family members to make informed, intentional decisions about their online behavior. This will create a sense of personal accountability and ownership.

Building Trust in External Expertise: Leverage trusted advisors or security professionals to guide safe digital practices. This external perspective helps reinforce best practices while allowing the family to focus on their priorities.

Adopting a Holistic Security Philosophy: Approach digital safety as part of a broader security and wellness framework, recognizing that physical, emotional, and digital well-being are interconnected. Encourage decisions that balance privacy with meaningful connections.

When companies offer proactive encouragement and support, executives and their families can create a sustainable and resilient approach to digital safety that aligns with their personal and professional needs. This shifts the focus from a prescriptive checklist to a thoughtful and adaptable way of engaging with the digital world.



Bit
Classical Computing

Qubit
Quantum Computing

WHAT IS A QUANTUM COMPUTER?

DR. EDWARD AMOROSO, SENIOR ANALYST, TAG

A quantum computer uses quantum bits called qubits. Unlike the binary digits in a classical computer, qubits can exist in a superposition, which means they can represent both 0 and 1 simultaneously. This property allows quantum computers to process many possibilities at once, exponentially increasing their computational power for specific problems. The following four concepts illustrate how a quantum computer can be used for computation:

1. **Superposition:** As suggested above, superposition is the ability of a qubit to be in multiple states (0 and 1) at the same time. For example, two classical bits can only be in one of four states (00, 01, 10, or 11) at a time. However, with two qubits, you can represent all four states simultaneously. This exponential scaling means that quantum computers can handle tasks such as optimization and search much faster than classical computers.

2. **Entanglement:** Entanglement is a phenomenon in quantum mechanics where qubits become strangely correlated in such a way that the state of one qubit is directly related to the state of another, regardless of the distance between them. This non-intuitive situation allows for faster transmission of information and enables quantum algorithms to perform certain computations that are infeasible for classical systems.

3. **Quantum Interference:** Quantum algorithms use something called interference to amplify correct answers and cancel out wrong answers. This approach is done in a quantum computer through operations applied to the qubits that affect their probabilities of collapsing to a particular state when measured. The cracking of conventional cryptography is enabled by quantum interference.

4. **Quantum Gates:** Similar to logic gates in classical computers, quantum gates manipulate qubits. However, quantum gates can perform operations on superpositions, allowing for much more complex transformations of data. Research teams at companies such as IBM are innovating the actual construction of systems that operate on this fundamental architectural approach to quantum computer implementation.

QUANTUM ALGORITHMS AND CRYPTOGRAPHY

Quantum computers, by leveraging the principles of subatomic quantum physics, offer a significant advantage in solving certain classes of mathematical problems more efficiently than classical computers. One area where quantum computing poses a substantial threat is cryptography, particularly with regard to the most widely used encryption algorithms today.

Shor's Algorithm: Classical cryptography relies on the difficulty of factorizing large integers (RSA—Rivest-Shamir-Adleman—algorithm) or solving discrete logarithms (ECC— Elliptic Curve Cryptography). These problems are computationally infeasible for classical computers due to the exponential time required as the key sizes increase. However, Shor's quantum algorithm can factor large integers and compute discrete logarithms in polynomial time, rendering RSA, ECC, and similar public-key cryptosystems insecure. A quantum computer with enough qubits (i.e., perhaps millions) could break these schemes, which are foundational to HTTPS, SSL/TLS, and digital signatures.

Grover's Algorithm: Symmetric key cryptography, such as AES, is more resistant to quantum attacks, but still vulnerable. Grover's algorithm allows a quantum computer to search an unsorted database more efficiently, effectively halving the security of symmetric key cryptographic systems. For instance, AES-256, which is currently considered secure, would offer only the equivalent of AES-128 security against a quantum computer using Grover's algorithm. This is still relatively secure but suggests that future encryption standards will need larger key sizes to maintain long-term security.

QUANTUM COMPUTING CHALLENGES AND CRYPTOGRAPHY'S FUTURE

While quantum computers currently face significant practical engineering challenges such as error rates, qubit coherence time, and scaling, their potential for advancing cryptographic attacks has led to the development of post-quantum cryptography (PQC). These algorithms are designed to be resistant to both classical and quantum attacks, ensuring security even as quantum technology advances.

At TAG, we believe that conventional cryptography is probably more vulnerable to the quantum threat than is normally reported, given the capability that most nation-states have with respect to both cryptography research and the construction of brute-force systems. That said, all companies should plan for a major technology and infrastructure transition to PQC sometime in the next decade.

BREACHRX

BreachRx is the first intelligent incident response platform that provides operational resilience for the entire enterprise. Its patented technology automatically generates tailored incident response plans and guidance for all stakeholders. Integrated privileged communications and audit trails ensure compliance with rapidly evolving regulations and standards to proactively protect CISOs from personal liability.

TAG
DISTINGUISHED VENDOR

REPRINTED FROM THE TAG SECURITY ANNUAL