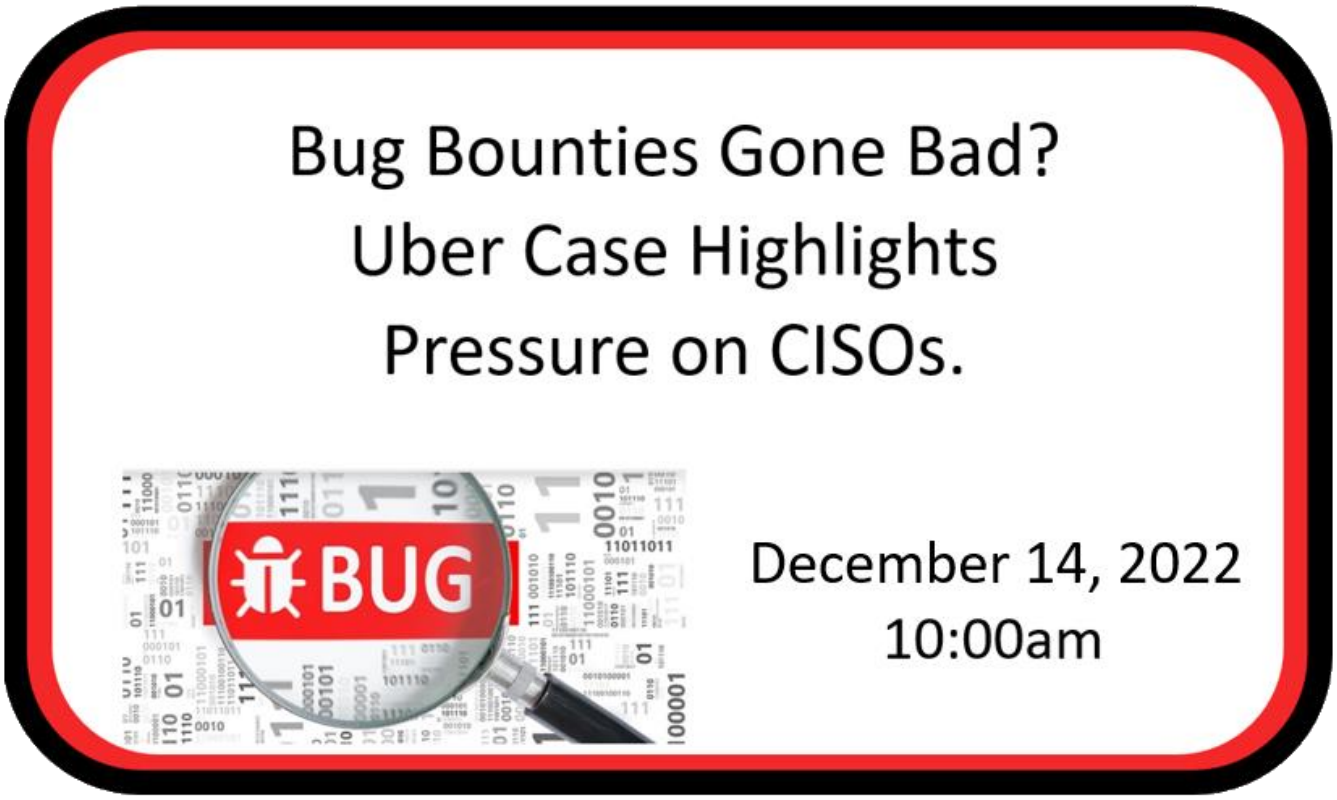
G2M RESEARCH

AI & Cybersecurity Newsletter

November 2022

Highlights



Bug Bounties Gone Bad?
Uber Case Highlights
Pressure on CISOs.

December 14, 2022
10:00am

Biden Administration Targets 4 Critical Infrastructure Sectors in Cybersecurity Reform

The Biden administration is focusing on four critical infrastructure sectors in its effort to reform the United States Cybersecurity Guidelines. The United States is looking to bolster its cybersecurity posture. In September, the Biden administration announced its first of a kind $1B State and Local Cybersecurity Grant Program (see G2M September Cybersecurity Newsletter) that was made possible by the Bipartisan Infrastructure Law that was passed in 2021. However, this funding is only one piece of the cybersecurity puzzle. The Colonial Pipeline hack that occurred in May of 2021 exposed vulnerabilities in America's cybersecurity defenses for critical infrastructure. Corporate IT functions should be partitioned from infrastructure IT, and they weren't in the Colonial Pipeline attack - bringing the company's functioning to a standstill until it paid the $4.4M ransom.

Transportation, Communications, Water and Healthcare are the four critical infrastructure sectors that the Biden administration is looking to bolster:

Our societies, and the critical infrastructure that supports them, from power to pipelines, is increasingly digital and vulnerable to disruption or destruction via cyber attacks. Such attacks have been used by countries, such as Russia, to undermine countries' ability to deliver services to citizens and coerce populations. We are working closely with allies and partners, such as the Quad, to define standards for critical infrastructure to rapidly improve our cyber resilience, and building collective capabilities to rapidly respond to attacks. - Biden-Harris Administration's National Security Strategy

The White House met with rail, maritime, aviation and pipeline executives over the summer to incorporate their feedback into the cybersecurity directive, which is expected to be released to the public soon. The Federal Communications Commission just finalized a rule for applying its new Mandatory Disaster Response Initiative to wireless network providers. The Environmental Protection Agency plans to creatively use sanitation review rules that are already on the books and include cybersecurity as a metric measured by these tests. Finally, the Department of Health and Human Services will be coming out with cybersecurity guidelines for hospitals, with rules for medical devices to follow. Connected medical devices, and IOT devices in general, is an emerging frontier for cybersecurity that likely will need standards for what security features IOT devices will need in order to protect against edge intrusion.

The executive branch continues to move forward using its executive powers to tighten regulations on private companies that operate in the critical infrastructure space, as there is gridlock in Congress in moving forward with new regulations. Trade associations for companies across the critical infrastructure sectors wrote to the Senate Armed Forces Committee and the Senate Homeland Security Committee expressing their opposition to the proposed legislation.

While the Biden Administration does have the authority to use executive privilege as it concerns critical infrastructure, it does not have the authority to regulate cybersecurity in the important Information Technology sector, where Congress would be required to step in and pass legislation to regulate cybersecurity.

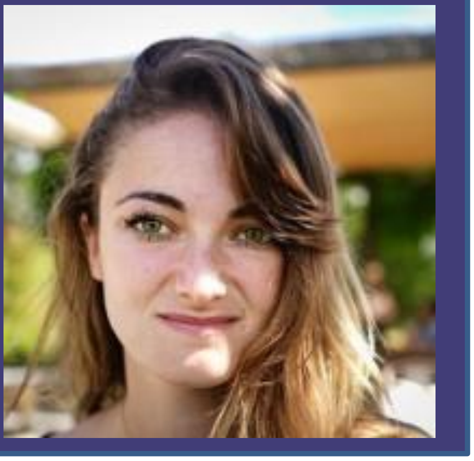
Steal Now, Decrypt Later

How Quantum Computing Could Unlock 2048-Bit Cryptography

With the promise of quantum computing comes incredible computing power and hyper-efficient algorithms that are built to leverage quantum computing's linear algebra-based vector spaces. In contrast to binary logic, quantum computing's fuzzy logic allows for multiple possible truth values to be processed through the same variable - with values ranging anywhere from (and in between) 0 to 1. This allows for the representation of concepts that are sometimes true or sometimes false. Through the use of several different fuzzy logic variables, cross product vector spaces are created, and event possibilities often emerge from these vector spaces with high certainty values. Additionally, these vector spaces can be used with vector based algorithms that can solve decryption problems much more efficiently then computers today that use binary logic.

One way of conceptualizing the difference between binary and quantum computing is to imagine that you are traveling through a maze. While binary computers have to choose which direction to go through the maze, and go through the maze some quantity of times before they figure out the optimal route through the maze, quantum computers can go in all of the possible directions at once:

> *“If you’re a quantum computer and you enter that maze, you don’t have to pick, you can go both ways at once,” she said. “And then with the quantum algorithm side, that cleverness is how you chop off the path that is not the most optimum path through the maze. “So what you’re left with in the end is this instantaneous, optimum path.”*
> *Rebecca Krauthamer, cofounder of QuSecure - a post-quantum cybersecurity firm*



The incredible scalar power that quantum computing allows for creates the possibility of solving problems that might take millions of years using binary logic on a traditional computer. Included in this possibility is the ability to decrypt 2048-bit numbers. 2048-bit cryptography is standard today, and encrypted files use a unique 2048 bit (617 digit) number. The factorization of this unique 617 digit number is the decrypt key that allows for access to the encrypted file.

To give everyone an idea of the scale of a 617 digit number, I created an easily factorable number that is close to 617 digits (my number is 618 digits). The number is a 25 digit number raised to the 25’th power. For reference, a 25 digit number is a septillion (10^24) - preceding septillion is sextillion (10^21), then quintillion (10^18), then quadrillion (10^15), then trillion (10^12), then billion (10^9).

My 25 digit number has a lead digit of 5 followed by 24 zeros:
5,000,000,000,000,000,000,000,000

Creating a 618 digit from this number requires raising it to the 24’th power:

5,000,000,000,000,000,000,000,000 ^ 24 =

298,023,223,876,953,125 * 10^600 =

**298,023,223,876,953,125,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,00
0,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,
000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,00
0,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,
000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,00
0,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,
000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,00
0,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,
000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000**

Factoring a 617 digit number, with all sorts of random digits, where the number doesn't easily factor as in my example, is incredibly, incredibly difficult - and time consuming. 617 digit numbers that are intelligently chosen (chosen to use factors that do not allow for easy brute-force algorithmic attack) would take more time to decrypt using today's computing power than the lifespan of the universe. Estimates are somewhere around 300 trillion years.

So the claim that quantum computing will be able to crack these types of codes in the future should be taken with a grain of salt. It will require significant quantum computing power, resources which likely will not be readily available to the public for at least a decade or two - and capabilities that do not exist today. But cross product vectorization spaces do allow for considerably greater scale than the (2^x) scale present in binary computing logic due to qubits and their ability to simultaneously occupy multiple positions. Using Shor's algorithm, problems such as the factorization of a 617 digit number get reduced to polynomial complexity (a number N raised to a number power, in my example my 25 digit number N was raised to the 24'th power), instead of exponential complexity - ex. 2^N.

A quantum computer with 4099 perfectly stable qubits could break the RSA-2048 encryption in 10 seconds (instead of 300 trillion years – wow). Quintessence Labs

Steal Now, Decrypt Later

Future Decryption Of Data Is A Liability

While quantum computing is still in its infancy, it will soon be able to quickly crack large numbers that classical binary computing will not be able to touch. When it does, 2048-bit data files will be vulnerable to decryption. Of course, when quantum computing becomes close to cracking 2048-bit encryption, then we can switch to a higher bit encryption system, or an encryption system that's based on quantum computing - that is what the future holds for cryptography. However, changing cryptography standards *in a decade or so* doesn't help governments and companies who have already had their encrypted data exfiltrated *today, tomorrow, or five years from now*. This is where the hacking strategy of Steal Now, Decrypt Later comes from - and is believed to already be in use today.

According to Dustin Moody, a mathematician at NIST, adversaries and nation-states are likely stealing and holding on to data until they can crack it later with quantum computers. Governments are aware of *the threat of a “keep to crack later” strategy. They’re taking even the slightest chance of this strategy being real very seriously and are working hard to develop quantum-safe algorithms. - Quantropi*

One important thing to remember about the Steal Now, Decrypt Later hacking approach is that it requires data that has a long shelf life. Consumer data from a decade or two ago may not be of value. Addresses change, and so do credit card numbers - and people cancel and open up new cards as well. Some consumers may not even be alive or living in the same state as they were a decade or two ago! Sensitive military and government documents however, tend to have a very long shelf life. Information of low importance is often declassified after a decade. Most US government documents are automatically declassified after 25 years. Narrow exemptions can be made for portions of US government documents that are of a national security interest, allowing for them to stay classified for 50-75 years. The implications of releasing these documents include revealing undercover operatives, clandestine operations, and both domestic and international top secret programs. Or alternatively, there may be classified documents that could be embarrassing to public figures such as former or current Presidents, Congressmen, and/or Diplomats.

Defense contractors also frequently hold sensitive information pertaining to military weapons, vehicles, ships and airplanes, and the technology built into them. As US military equipment can be in use for 30-40 years, the information contained in these units’ technical documentation can be valuable for the lifespan of the military vessel or weapon. Steal Now, Decrypt Later represents a strategic threat to US military superiority. The information gleaned from these engineering documents could be used to manufacture their own versions of our military equipment, disarm or disable our military equipment, and find and exploit weaknesses in our military equipment. The same principles apply not just to US military equipment, but also other NATO countries’ military equipment.

In order to counter the impending ‘quantum apocalypse’, the US National Institute of Standards and Technology is in the process of implementing a quantum-resistant cybersecurity standard. The NIST initiative to devise new encryption algorithms began in 2016, and the NIST has selected four encryption algorithms that it believes can withstand an attack from a quantum computer in the future. This new NIST standard is expected to be formalized by 2024. Organizations that want to begin the transition process now are urged to follow the CISA’s Post-Quantum Cryptography Roadmap.

Our post-quantum cryptography program has leveraged the top minds in cryptography – worldwide – to produce this first group of quantum-resistant algorithms that will lead to a standard and significantly increase the security of our digital information. - NIST director Laurie E. Locascio

Improving Organizational Cybersecurity

What can organizations do to improve their cybersecurity posture?

Educate all employees on security

Protecting the edge is partly about ensuring that the edge users (ie. your employees) are following cybersecurity best practices. These include:

- Ensuring that all passwords are durable and changed routinely
- Using password screen-locking and device tracking for all mobile devices
- Don't give out personal information, usernames or passwords when asked via email
- 46% of cybersecurity leaders target improved security awareness training as something that they would like to invest in if they had more funds available.
- *82% of breaches involved the human element, including Social Attacks, Errors, and Misuse. - Verizon Data Breach Report*

Create Cybersecurity and IT Assistant Positions

Cybersecurity is facing a severe labor shortage. Many jobs go unfilled. Even worse, job stress is causing many employees to leave the field. Not to mention, if your company is hacked into, the stress associated with mediating the breach and recovering data and business operations is sure to lead to employee fatigue, more time off, and/or resignations. Creating new assistant positions:

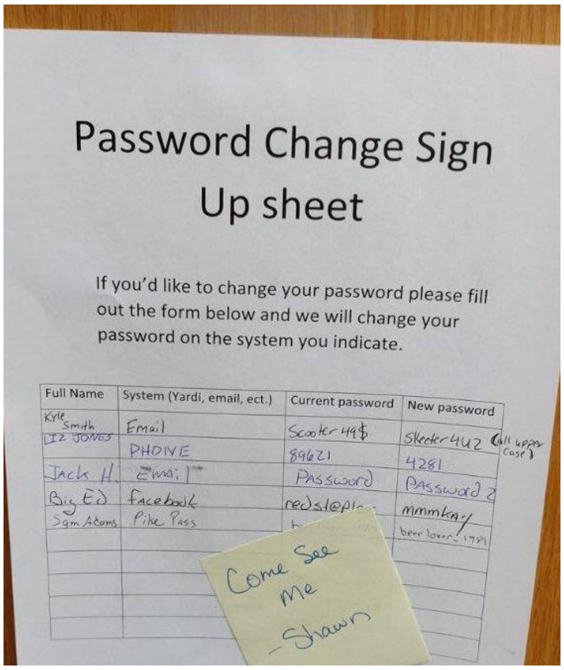
- Allows Cybersecurity and IT employees to assign general office tasks to assistants that do not require a high level of IT or Cybersecurity knowledge
- Allows Cybersecurity and IT employees to be more productive and less stressed
- Allows assistants to develop Cybersecurity and IT knowledge, building human capital in a field that cannot meet hiring demand with jobseeker supply
- Provides for more 'hands on deck' in case of a cybersecurity breach

In November 2018, the InfoSec Institute polled 785 IT and security professionals on career-related questions. When asked which work-related issue keeps them up at night, 12% said they had too much work but not enough staff to help with it all.

Provide IT and Cybersecurity Employees With Wellness Resources

Securing your company's cybersecurity can be stressful, especially at the executive level. The burden of protecting your company's information and operational ability is dependent upon stopping threats that you can't see or hear coming. The 24/7/365 threat of a breach can take an emotional and psychological toll on anyone that works in this field. The best approach for companies to take in order to ameliorate this is a proactive one:

- Encourage Cybersecurity and IT employees to find a counselor or therapist that they can talk to on a regular basis *before* a breach occurs! Both the threat of a breach and a breach itself are stressful events. Having a support network in place beforehand will not only improve employee morale, but also increase employee retention after a breach.
- Provide a short amount of time in the day for Cybersecurity and IT employees to disconnect from job tasks and de-stress. This could be 15 minutes of meditation, breath work, and/or yoga poses. Or it could be 15 minutes of listening to music, or going for a walk outside.
- Encourage employees to use their sick leave! America in particular has a work culture that incentivizes 80 hour work weeks and outworking your peers in order to prove yourself. Create a corporate culture that promotes work-life balance.
- *One-third (33%) of cybersecurity decision-makers are thinking of leaving their role in the next two years due to stress or burnout. -* *Mimecast Report*



Password Change Sign Up sheet

If you'd like to change your password please fill out the form below and we will change your password on the system you indicate.

Full Name	System (Yardi, email, ect.)	Current password	New password
Kyle Smith	Email	Scooter49$	Skeeter442 (all upper case)
LIZ JONES	PHONE	89621	4281
Jack H.	Email	Password	Password2
Big Ed	Facebook	redsl@pl	mmmkay/
Sam Adams	Pike Pass	b	beer lover 1981

Come See Me
-Shawn

Have a Plan in Place In Case the Company is Attacked

Creating a security breach plan is useful for a number of reasons:

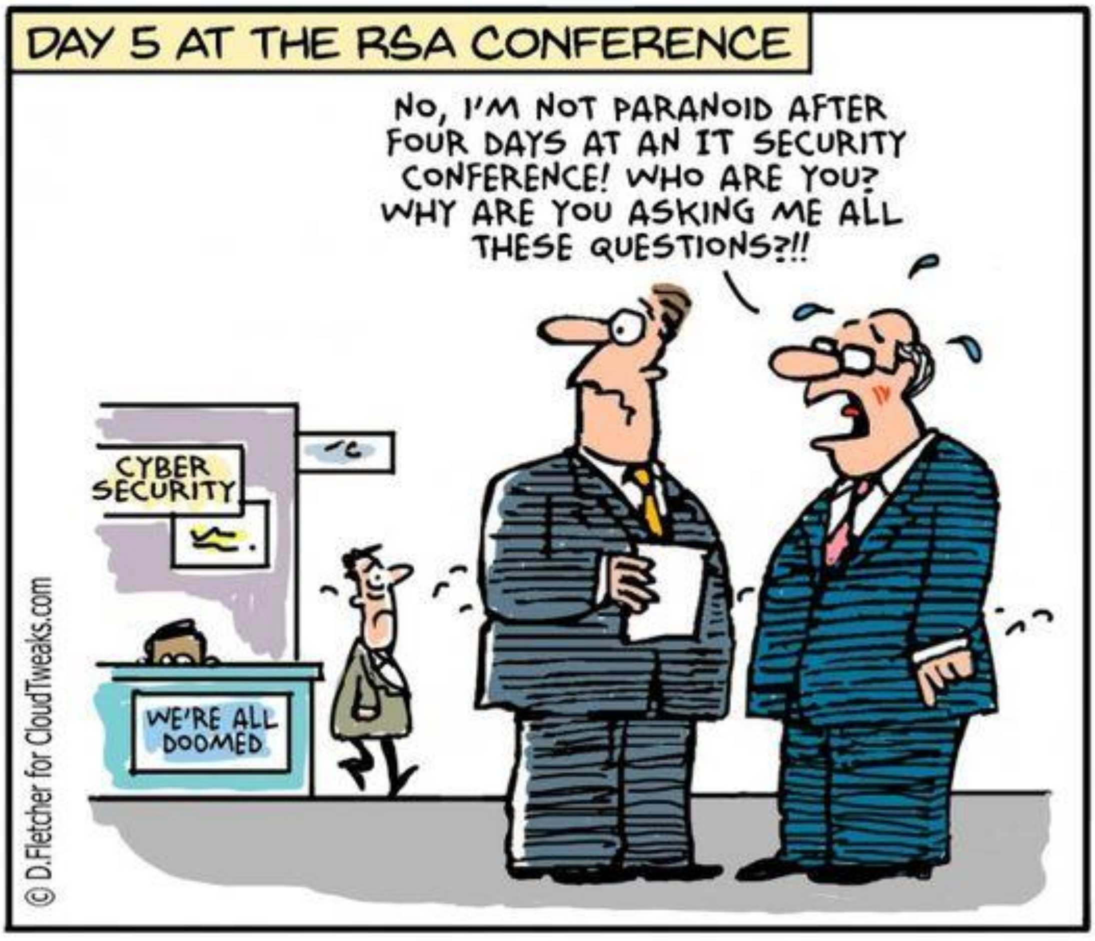
- Creating a plan is useful because it is a brainstorming exercise that will help you to come up with both better cybersecurity defenses.
- Creating a plan will lead to the identification of choke-points in the crisis response. One example of this is how a breach can often paralyze company communications by shutting down email services, greatly harming company productivity.
- Security breaches are stressful events. Under heightened stress, people have a tendency to shut down neurologically, and critical thinking skills suffer. Having a plan already in place allows taxed decision-makers to have a starting point to fall back on in their response to the threat.

- Not having a cybersecurity breach plan can be incredibly expensive. Businesses with an IR (Incident Response) team that tested its IR plan saw an average of USD $1.29M lower breach costs than organizations without an IR team and that don’t test an IR plan.

Invest More Money into Cybersecurity and IT Budgets

Cybersecurity suffers from underfunding, and the rise of ransomware attacks has only made the problem worse. Investing more money into upgraded cybersecurity defenses pays for itself:

- 94% of cybersecurity leaders believe more budget is required to combat ransomware, identifying an incremental budget boost of 28% on average
- Nearly two-thirds (64%) of cybersecurity leaders have experienced at least one ransomware attack in the past year
- A single ransomware attack can consume a significant portion of the cybersecurity budget itself. Reaching an all-time high, the cost of a data breach averaged USD 4.35 million in 2022.
- 59% of organizations don’t deploy a zero trust architecture. Organizations with zero trust deployed saved nearly USD 1 million in average breach costs compared to organizations without zero trust deployed.
- 46% of cybersecurity leaders say that they need up-to-date security systems.
- Breaches at organizations with fully deployed security AI and automation cost USD 3.05 million less than breaches at organizations with no security AI and automation deployed. 30% of organizations today do not use security AI and automation.


DAY 5 AT THE RSA CONFERENCE
NO, I'M NOT PARANOID AFTER FOUR DAYS AT AN IT SECURITY CONFERENCE! WHO ARE YOU? WHY ARE YOU ASKING ME ALL THESE QUESTIONS?!!
CYBER SECURITY
WE'RE ALL DOOMED
© D.Fletcher for CloudTweaks.com

G2M Research Multi-Vendor Webinar Series

Our webinar schedule is below. Registration links and more information will be available in our next newsletter, on our website, and you can always contact us directly with questions. We are offering a Cybersecurity series and an Enterprise Storage & Technology multivendor series.

Interested in Sponsoring a webinar? Contact G2M for a prospectus. We can create custom webinar, custom webinar series, and add or modify topics to specifically appeal to your target audience. View our webinars and access slide deck presentations on our website.

Cybersecurity

Bug Bounties Gone Bad? Uber Case Highlights Pressure on CISOs.	December 14
Key Cybersecurity Trends for 2023	January 12
Cybersecurity for Remote Workers & Mobile Devices	February 23
The Increasing Complexity of Cybersecurity Regulatory & Compliance for the Financial Services Industry	March 23
Beyond the CISO Organization – Meeting the Cybersecurity Needs of the C-Suite & Boardroom	May 4
Cybersecurity- Finding, Training, & Retaining the Best Talent	May 25
xDR- The Promise versus the Reality	June 15
HIPAA, GDPR, Data Privacy, & Cybersecurity- 5 Keys to Make It All Work Together	July 13
Beyond Ratings – 5 Things You Can Do With a Third Party Risk Management (TPRM) Program	August 17
10 Features of an Effective Attack Surface Management Tool	September 7
How Secure is the Cloud for Your Workloads?	October 12
Do You Need a SIEM? Use Cases Where a SIEM Makes Sense.	November 9
Cybersecurity Predictions for 2024	December 7

Enterprise Storage & Technology

OCP 2022 Wrap Up – The Latest and Greatest in SSDs, CXL, Accelerators, and Other Big Trends for the Datacenter and the Cloud	November 15
Storage Architectures for Artificial Intelligence & Machine Learning	February 7
Memory As The New Storage – CXL, Extended Memory, & Persistent Memory. What Does the Future Hold?	March 7
The Need for Speed: NMVe & Advanced SSDs	April 4
Software-Defined Flash Memory Architectures	May 9
Storage & Compute Architectures for Healthcare & Imaging Applications	June 27
NVMe & NVMe-oF – Past, Present, & Future (at FMS)	August 2
GPUs, SSDs, & Shared Memory: Accelerating Computing?	August 22
Securing Data – How Storage & Cybersecurity Technologies Can Work Together	Sept 26
The Open Compute Platform (OCP) Movement – Providing Compute-At-Scale Value to On-Premises Deployments	October 24
Storage Architectures for HPC Clusters	November 21
2024 Trends – Cloud, On-Premises, & Hybrid Compute/Storage	December 12

Upcoming Conferences

November 7-9	Acronis #Cyberfit Summit 2022, Miami, FL
November 7-10	VMWare Explore Europe, Barcelona
November 9-11	IT Nation Connect, Orlando, FL
November 13-18	SC22, Dallas
November 14-16	Gartner IT Symposium/Xpo India, Kochi, India
November 14-17	Titanium Converge, Austin, TX & Virtual
November 15-17	Black Hat Middle East & Africa 2022, Saudi Arabia
November 15-17	ISC East, NYC
November 16	San Diego Cybersecurity Conference, Hybrid
November 16	Threat Hunting Summit, Virtual
November 18-19	Data Strategy & Insights (Forrester Research), Virtual
November 21-22	Gartner IT Infrastructure, Operations, & Cloud, London
November 28-Dec 2	AWS re:Invent, Las Vegas
December 1-2	Digital Transformation Expo Global, London
December 5-6	Healthcare Cybersecurity Forum, Boston, MA
December 5-8	Black Hat Europe 2022, London

December 6	Security Operations Summit, Virtual
December 6-8	Gartner IT Infrastructure, Operations & Cloud, Las Vegas
December 6-9	Cisco Live, Melbourne, Australia
December 10-14	Edge 2022: International Conf on Edge Computing, Hawaii
December 10-14	Cloud 2022: International Conf Cloud Computing, Hawaii
December 12-15	Palo Alto Networks Ignite, Las Vegas
December 13	Black Hat Cybersecurity Outlook 2023, Virtual
2023	
January 5-8	CES, Las Vegas & Virtual
January 18	SNIA Persistent Memory Summit, San Jose, CA
January 30-Feb 1	Cybertech Global TLV, Tel Aviv, Israel
February 6-10	Cisco Live, Amsterdam, Netherlands
February 13-14	Gartner Security & Risk Management, Mumbai, India
February 14-16	ESNA Expo, Long Beach, CA
February 14-17	ITExpo East, Fort Lauderdale, FL
February 27-28	Gartner Security & Risk Management Summit, Dubai
February 27-March 2	Mobile World Congress Barcelona
February 28-March 2	Rice University Energy HPCC Conference, Houston, TX
March 8-9	CloudExpo Europe, London
March 14-16	Gulf Information Security Expo, Dubai, UAE
March 20-22	Gartner Data & Analytics Summit, Grapevine, TX
March 20-23	GTC CPU Technology Conference, San Jose, CA
March 28-29	Gartner Security & Risk Management, Sydney, Australia
March 28-31	ISC West, Las Vegas
April 5-7	IST Information Security Expo, Tokyo, Japan
April 15-19	NABShow, Las Vegas
April 17-21	HIMMS Global Health Conference, Chicago, IL
April 19-20	CyberSec Europe, Brussels, Belgium

April 24-27	RSA Conference, San Francisco
May 22-25	Dell World, Las Vegas
June 2-6	School Transportation Network Expo East, Indianapolis, IN
June 4-8	Cisco Live, Las Vegas
June 5-7	Gartner Security & Risk Managemnt, National Harbor, MD
June 7-9	Synnex Red, White and You, Greenville, SC
June 14-16	Interop Tokyo, Chiba, Japan
June 20-22	HPE Discover, Las Vegas
June 20-22	Info Security Europe, London
July 14-19	School Transportation Network Expo, Reno, NV
August 1-3	Flash Memory Summit, Santa Clara, CA
August 5-10	Black Hat USA, Las Vegas
August 30-Sept 1	Security Expo, Sydney, Australia
September 11-13	Gartner Security & Risk Management, London
September 11-13	Global Security Exchange, Dallas, TX
September 18-20	Crowdstrike fal.con, Las Vegas
October 2-4	DattoCon, Miami, FL
October 3-4	CyberTech Europe, Rome

G2M RESEARCH

Effective Marketing & Communications
with Quantifiable Results