2023

THE CISO'S ANNUAL PLANNER

Survive and thrive in the age of unpredictability with this 12-month cybersecurity calendar

CXO REvolutionaries

SPONSORED BY: zscaler

Dear CISO,

As someone with a role increasingly in the spotlight, we know your day-to-day responsibilities such as securing your organizational information assets, managing the SOC, leading people, and keeping the business up to speed about evolving risks is not easy. To help you, this 12-month challenge includes strategies, tips, and advice for issues and concerns already on your plate. The goal is to get you organized and put you in a great position to exit 2023 as a/an:

- Trusted advisor to the C-suite and board of directors
- Internal and external security expert
- Authority on the highest level of security you can afford
- Protector that keeps the organization out of the headlines due to a breach
- Collaborator who enables the business rather than create barriers

This planner includes monthly challenges that you can follow or modify to suit your unique environment. Some could take months or a full year, whereas others may be divided up. For example, some incident response plans can be technical and others focused on executives, so you may do both but at different periods of the year. Choose initiatives that are right for you.

Save this PDF and create a photocopy to put alongside your calendar and consult it often to stay on track with your goals.

Please share any feedback to **cxo@zscaler.com**

We hope you find it useful and that your 2023 is successful!

Sincerely,
Christopher Jablonski
Director, CXO REvolutionaries & Community

12-MONTH CHALLENGE AT-A-GLANCE

Q1

SET UP YOUR FOUNDATION

- JAN Threat landscape ▸
- FEB Cyber risk assessment ▸
- MAR NIST Cybersecurity Framework ▸

Q2

BUILD RESILIENCE

- APR Incident response plans ▸
- MAY MITRE ATT&CK ▸
- JUN Disaster recovery and business continuity ▸

Q3

GAIN INFLUENCE

- JUL Board-level communications ▸
- AUG Industry events plus R&R ▸
- SEP 2024 annual budget ▸

Q4

BOOST AWARENESS AND CYBER PROFICIENCY

- OCT Cybersecurity awareness month ▸
- NOV The 18 CIS Critical Security Controls ▸
- DEC CISA Cross-Sector Cybersecurity Performance Goals ▸

JANUARY / 01

1	SUN	New Year's Day
2	MON	
3	TUE	
4	WED	
5	THU	CES
6	FRI	CES
7	SAT	CES
8	SUN	CES
9	MON	
10	TUE	
11	WED	
12	THU	
13	FRI	
14	SAT	
15	SUN	
16	MON	Martin Luther King Day
17	TUE	
18	WED	
19	THU	
20	FRI	
21	SAT	
22	SUN	
23	MON	
24	TUE	
25	WED	
26	THU	
27	FRI	
28	SAT	Data Privacy Day
29	SUN	
30	MON	
31	TUE	

YOUR CHALLENGE

THREAT LANDSCAPE

Happy new year! The business of risk management has steadily been cascading from directors down to implementation teams. CISOs like you need to stay informed and be proactive as your role constantly evolves. Managing risk with one eye on the shifting cybersecurity landscape is the central challenge you face.

That means that if you are a seasoned executive or a new CISO, you must continually align your organization's cybersecurity program with top threats, new policies, frameworks, CIO or board requirements, industry standards, and, of course, the demands of end users.

But don't do it all at once. You have a million things going on right now. So for this month, just research the causes of risk by **conducting extensive research on the threat landscape of your industry**. The experts from the Office of the CISO at Zscaler can help you (Get in touch).

When playing a game on a field with no boundaries and no goal line you can never declare victory. The way forward for managing risk is to mutually come to terms with leadership on what to focus on because you only have a finite number of hours in the day.

To understand your total risk surface area and the parts that are more critical than others, you need to know what the threat landscape looks like from cybercrime through to other forms of business risk, be it operational, loss of intellectual property, supply chain, and macroeconomic. From there, you are ready to perform a cyber risk assessment.

ACTION ITEMS

- [ ] Document and present your threat landscape
- [ ] Review and update your incident response contact list
- [ ] Review and update policies
- [ ]
- [ ]
- [ ]
- [ ]

NOTES

FEBRUARY/02

1	WED	
2	THU	
3	FRI	
4	SAT	
5	SUN	
6	MON	
7	TUE	ENISA Cybersecurity Standardisation Conference 2023 – Brussels
8	WED	
9	THU	
10	FRI	
11	SAT	
12	SUN	
13	MON	
14	TUE	Valentine's Day
15	WED	
16	THU	Zscaler Global CISO Exchange – Miami
17	FRI	Zscaler Global CISO Exchange – Miami
18	SAT	
19	SUN	
20	MON	President's Day
21	TUE	
22	WED	
23	THU	
24	FRI	
25	SAT	
26	SUN	
27	MON	Gartner Security & Risk Management Summit – Dubai
28	TUE	Gartner Security & Risk Management Summit – Dubai

YOUR CHALLENGE

CYBER RISK ASSESSMENT

It's time to take a deep look at your organization's security strategies and capabilities. Once you can **measure your ability to protect your information and information systems from cyber threats**, you are in a position to take action. Think of the output as a roadmap for successful security outcomes based on objectives, priorities, and targets developed, in part, from your research into your threat landscape.

When implementing or updating your organization's current or future security strategy, you should consider cost/resource justification, complementary or non–technical control coverage, control/compliance relationships, and alignment to business security goals

Evaluate your status and capabilities for each of the following key categories: threat and data protection; zero trust architecture; cloud workload and application security; user experience; governance, risk, and compliance; and, security operations.

Performing a detailed assessment and completing it could take all year, so we put one of the the most popular risk assessment frameworks available, National Institute of Standards and Technology (NIST) Cybersecurity Framework as the focal point for March. Best to get started now. You can use it, or ISO/IEC 27001:2022, create your own, or have the experts from the Office of the CISO at Zscaler help you (Get in touch).

Join us for the CISO Exchange in Miami.

ACTION ITEMS

- [ ] Launch a cyber risk assessment initiative
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]

NOTES

MARCH/03

1	WED	Women's History Month
2	THU	
3	FRI	
4	SAT	
5	SUN	
6	MON	
7	TUE	
8	WED	International Women's' Day
9	THU	
10	FRI	
11	SAT	
12	SUN	Daylight Savings Time starts
13	MON	
14	TUE	
15	WED	
16	THU	
17	FRI	St. Patrick's Day
18	SAT	
19	SUN	
20	MON	
21	TUE	
22	WED	
23	THU	
24	FRI	
25	SAT	
26	SUN	
27	MON	
28	TUE	
29	WED	
30	THU	
31	FRI	

YOUR CHALLENGE

NIST CYBERSECURITY FRAMEWORK

The smart folks over at NIST pieced together nearly a half dozen standards to create the NIST Cybersecurity Framework (NCSF), a "voluntary guidance, guidelines, and practices to help organizations better manage and reduce cybersecurity risk," as they explain. It is the framework of choice among the majority of large enterprises, who reference and incorporate it into their programs.

It is divided into five "functionalities," which are further divided into 23 "categories." There are 108 subcategories in all, one for each of the cybersecurity outcomes and security controls. The functionalities include: Identify, Protect, Detect, Respond, Recover.

Get yourself a copy of the NIST Cybersecurity Framework and disseminate for review. Then schedule a discussion on this topic for your next formal cybersecurity planning session, and over the next three months, map the CSF core against your existing risk and cybersecurity controls and identify gaps and opportunities for improvement. Over the year, adopt those elements of the NIST CSF (in part or whole) into your corporate risk and cybersecurity approach where applicable. Finally, build an organizational framework that is based on CSF and use it as a guide moving forward for continuous improvement.

If using another framework follow the prescribed adoption and maturity process. Regardless, document your strategy.

ACTION ITEMS

- [ ] Deliver first component of your cyber risk assessment
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]

NOTES

APRIL/04

1	SAT	
2	SUN	
3	MON	
4	TUE	
5	WED	
6	THU	
7	FRI	
8	SAT	
9	SUN	Easter
10	MON	
11	TUE	
12	WED	
13	THU	
14	FRI	
15	SAT	
16	SUN	
17	MON	
18	TUE	
19	WED	
20	THU	
21	FRI	
22	SAT	
23	SUN	
24	MON	RSA Conference 2023
25	TUE	RSA Conference 2023
26	WED	RSA Conference 2023
27	THU	RSA Conference 2023
28	FRI	
29	SAT	
30	SUN	

YOUR CHALLENGE

INCIDENT RESPONSE PLANS

Benjamin Franklin once said that “By failing to plan, you are preparing to fail.” This famous adage hits home hard for cybersecurity leaders. Your incident response (IR) plan should help you and your organization respond and recover from a cyberattack or a crisis stemming from a cyber incident should one happen on your watch.

Pay close attention to what you detail in the “Golden Hour,” which the **Cyber Management Alliance** explains as the during-an-incident period that entails knowing who you are going to call, who can authorise critical actions, who handles the press, the third-party that will handle forensics, the members of the crisis management team, and so on. You also need a similar post-incident playbook.

Verify your contact list and update procedures and your playbooks.

Tabletop exercises (TTXs) are a great way to assess your plan and can reveal whether your organization can handle a specific class of attack. Practicing critical decisions within the C-suite provides vital intel needed to optimize reactions to potential incidents. It’s better to debate response efforts when not in the middle of an attack.

Drilling your IR plan frequently and thoughtfully will help in a significant way to reduce conflict when tough decisions need to be made during a live incident and maximize efficiency when handling a real-life incident within your organization. There are many templates available online. Defending against attacks in the modern cloud era calls for a common framework to understand how attackers operate to achieve their objectives.

ACTION ITEMS

- [ ] Review and update your IR plan and contact list
- [ ] Review and update standards
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]

NOTES

MAY'05

1	MON	First Day of Asian Pacific American Heritage Month
2	TUE	
3	WED	
4	THU	
5	FRI	Cinco de Mayo
6	SAT	
7	SUN	
8	MON	
9	TUE	Black Hat Asia
10	WED	Black Hat Asia
11	THU	Black Hat Asia
12	FRI	Black Hat Asia
13	SAT	
14	SUN	Mother's Day
15	MON	
16	TUE	
17	WED	
18	THU	
19	FRI	
20	SAT	
21	SUN	
22	MON	
23	TUE	
24	WED	
25	THU	
26	FRI	
27	SAT	
28	SUN	
29	MON	Memorial Day
30	TUE	
31	WED	

YOUR CHALLENGE

MITRE ATT&CK

The MITRE Corporation developed a process for modeling an adversary's post-compromise behavior at a granular level with a common taxonomy. This model is named the ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework, and is a knowledge base of commonly observed adversarial behaviors to support the efforts of threat intelligence functions, with adversary emulation and defensive gap analysis.

The model describes the Tactics, Techniques, and Procedures (TTPs) of adversarial behavior and breaks them into categories based on the sequence of steps involved in an attack. It is not intended to be exhaustive and is very much a living framework that is continuously updated as new TTPs are discovered.

Nonetheless, ATT&CK is designed to help break down, classify, and document adversarial behaviors from previously observed attacks in a common language that is consistent and clear. This lets you test and verify your defenses; assess tools, monitoring, and mitigation capabilities of existing defenses; find security gaps; and, identify and rank alerts based on their potential threat level, among other benefits.

Read **ATT&CK 101** to get started and we recommend first pursuing **ATT&CK Matrix for Enterprise**. Already done? There's **MITRE Engage**. Questions? **Get in touch**.

ACTION ITEMS

- [ ] Master TTPs that afflict your industry and organization
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]

NOTES

JUNE/06

1	THU	
2	FRI	
3	SAT	
4	SUN	
5	MON	
6	TUE	
7	WED	
8	THU	
9	FRI	
10	SAT	
11	SUN	
12	MON	
13	TUE	Zenith Live – Las Vegas
14	WED	Zenith Live – Las Vegas
15	THU	Zenith Live – Las Vegas
16	FRI	
17	SAT	
18	SUN	Father's Day
19	MON	Juneteenth
20	TUE	
21	WED	
22	THU	
23	FRI	
24	SAT	
25	SUN	
26	MON	
27	TUE	Zenith Live – Berlin, Germany
28	WED	Zenith Live – Berlin, Germany
29	THU	Zenith Live – Berlin, Germany
30	FRI	

YOUR CHALLENGE

DISASTER RECOVERY AND BUSINESS CONTINUITY

Cyber incidents whether man-made, an act of nature, or technical failure can mean more than a few hours of downtime. The point is that here are many potential disruptive threats that can occur at any time and affect normal business processes. Disaster recovery (DR) and business continuity planning (BCP) build on your well-established incident response plans.

With everyone but you on vacation, you can carve out quiet time to accurately classify and update your roster of mission-critical assets, understand service providers' failover capabilities, and ensure every assets' resilience mirrors its criticality.

Based on assessments of acceptable risk, can your on-prem infrastructure and SaaS/PaaS be trusted to provide highly available service and rapid recovery from outages? Are cloud-based applications critical enough that alternative backup measures must be implemented?

As a CISO, consider what you will need to to help facilitate remote work, restore data, bring back connectivity, and handle a ransom. Imagine the worst case scenario. How long would it take you to completely rebuild your network? Think about the steps you would take, the order you would need to take them, your top priorities, and estimated timelines. Consider you infrastructure. Which assets are in the cloud? Which are virtual or hybrid? Where are your endpoints located? What does restoration look like? These are just some of the higher level points of what should be a detailed document laying out your DR/BC

ACTION ITEMS

- [ ] Update your DR/BC plan and role
- [ ] Semiannual update to your playbooks
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]

NOTES

JULY

1	SAT	
2	SUN	
3	MON	
4	TUE	Independence Day
5	WED	
6	THU	
7	FRI	
8	SAT	
9	SUN	
10	MON	
11	TUE	
12	WED	
13	THU	
14	FRI	
15	SAT	
16	SUN	
17	MON	
18	TUE	
19	WED	
20	THU	
21	FRI	
22	SAT	
23	SUN	
24	MON	
25	TUE	
26	WED	
27	THU	
28	FRI	
29	SAT	
30	SUN	
31	MON	

YOUR CHALLENGE

BOARD-LEVEL COMMUNICATIONS

Boards of directors must understand that cybersecurity is a dynamic discipline that requires unending monitoring and innovation. Laying the groundwork for reduced risk is essential but so is the knowledge that risk will always be there. Each board is unique, but they share something in common regarding risk: they understand things like credit, operational, and global risk. On the flip side, they rarely understand the risks associated with IT and digitalization. That's where you come in.

When you go to the board with your portfolio of projects, you may think yours are the highest priority. But you need to present it in the context of the total threat landscape that you're dealing with.

The board thinks they're investing $X million in security, and then they can't understand why the investment may not result in not being breached. By modeling the financials and risks correctly and laying out the worst-case scenarios in a manner that helps to prioritize, you help boards understand the probability and the likelihood of something happening and how bad it will be if it does. Stack rank and explain risks and threats to communicate the realities of how much of the risk surface area the proposed budget can cover (and what it does not).

You should also assess your existing cyber insurance policies, whether they adequately cover asset value in the event of a breach, and if dedicated cyber insurance may help further mitigate risk. Keep leadership involved and educated in cybersecurity for the business and prepare policies and procedures in the event of a breach with an eye toward responsibility.

ACTION ITEMS

- [ ] Refine your messaging and present it to the BoD
- [ ] Review and update your incident response contact list
- [ ] Review and update procedures
- [ ]
- [ ]
- [ ]
- [ ]

NOTES

AUGUST '08

1	TUE	
2	WED	
3	THU	
4	FRI	
5	SAT	Black Hat USA
6	SUN	Black Hat USA
7	MON	Black Hat USA
8	TUE	Black Hat USA
9	WED	Black Hat USA
10	THU	Black Hat USA | DEF CON 31
11	FRI	DEF CON 31
12	SAT	DEF CON 31
13	SUN	DEF CON 31
14	MON	
15	TUE	
16	WED	
17	THU	
18	FRI	
19	SAT	
20	SUN	
21	MON	
22	TUE	
23	WED	
24	THU	
25	FRI	
26	SAT	
27	SUN	
28	MON	
29	TUE	
30	WED	
31	THU	

YOUR CHALLENGE

INDUSTRY EVENTS PLUS R&R

Las Vegas heats up in August and so does the business of cybersecurity thanks to Black Hat (founded in 1997) and DEF CON (1993). 15 years ago the late Dan Kaminsky gave his seminal "Great DNS Vulnerability" keynote at Black Hat 2008. He exposed a fundamental DNS flaw that led to a multi-vendor, coordinated patch release. Chances of another gifted security researcher "saving the internet" again this year are slim but along with DC, expect headlines, surprises, and hacks as the conjoined confab just keeps getting bigger and bigger with more blending of attendee audiences than ever.

Now is a great time to open your team to training and certification opportunities such as in zero trust, and join communities and working groups such as those offered within the **Cloud Security Alliance**. Explore how you can help with cross-industry threat intelligence collaboration by contacting you sector's **ISAC - Information Sharing and Analysis Center**.

Equally important is to ensure your team has scheduled time off before end of the year. Taking care of your people is key. August is a popular time for family vacations before kiddos go back to school. Plan for coverage accordingly.

ACTION ITEMS

- [ ] Attend conferences
- [ ] Schedule PTO for you and your team if not already taken
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]

NOTES

SEPTEMBER/09

1	FRI	
2	SAT	
3	SUN	
4	MON	Labor Day
5	TUE	
6	WED	
7	THU	
8	FRI	
9	SAT	
10	SUN	
11	MON	
12	TUE	
13	WED	
14	THU	
15	FRI	
16	SAT	
17	SUN	
18	MON	
19	TUE	
20	WED	
21	THU	
22	FRI	
23	SAT	
24	SUN	
25	MON	
26	TUE	Gartner Security & Risk Management Summit – London, U.K.
27	WED	Gartner Security & Risk Management Summit – London, U.K.
28	THU	Gartner Security & Risk Management Summit – London, U.K.
29	FRI	
30	SAT	

YOUR CHALLENGE

2024 ANNUAL BUDGET

Around now the 2024 budgeting season gets underway depending on your fiscal year. Funds may be tight given the state of the economy, bust security is still top of the IT list. As a CISO you have bobbed the waves of the economy for many years. As a cost center within a business, that just seemed to be what you had to do. When times are good, you partner with the CIO to make technology investments. When they are tough, you sweat every technology you have. Tech debt simply grows and grows.

Proper budgeting and operational planning are mainly the domain of the CIO and CFO. IT and cyber teams are typically called on to do more with less without appropriate resources. Budgeting should have a two-fold emphasis: trim unwarranted or outdated expenses while spending in areas of the greatest potential return. Budgets have traditionally been set in stone from the onset of a year or fiscal calendar. CIOs make plans, allocate funds, and stick to the script. Before embarking on any proposed change in project funding our headcount conduct a full risk assessment of the program and status and translate the results into business impact to build consensus and support for the plan or budget. Create and update your roadmap.

A word to the wise fo new CISOs: most get stuck right away in firefighting mode and carry the ops and budget burden for in-flight projects and for what is already in place. They often lean into compliance as the “lever” to dislodge $$$. It works for a while but often leads to bad outcomes.

ACTION ITEMS

- [ ] Plan and prepare your annual budget
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]

NOTES

OCTOBER/10

1	SUN	Cybersecurity Awareness Month begins
2	MON	
3	TUE	
4	WED	
5	THU	
6	FRI	
7	SAT	
8	SUN	
9	MON	Columbus Day | Indigenous Peoples' Day
10	TUE	
11	WED	
12	THU	
13	FRI	
14	SAT	
15	SUN	
16	MON	
17	TUE	
18	WED	
19	THU	
20	FRI	
21	SAT	
22	SUN	
23	MON	
24	TUE	
25	WED	
26	THU	
27	FRI	
28	SAT	
29	SUN	
30	MON	
31	TUE	Halloween

YOUR CHALLENGE

CYBERSECURITY AWARENESS MONTH

At the time of the release of this planner, no theme was available yet for **Cybersecurity Awareness Month**, an initiative launched in 2004 by the President of the United States and Congress. The Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance (NCA) lead the effort between the public and private sectors to raise cybersecurity awareness nationally and internationally.

This is a great opportunity to remind your organization of the basics of cybersecurity and to renew vigilance to threats like phishing and social engineering attacks. Going beyond promoting the use of MFA, strong passwords, and updating software, CISOs can also spread awareness to leaders in the organization about risk management:

- Realize that you can't protect yourself from everything so accept risk but do prioritize what to de-risk
- Success is defined by the defensibility of your decisions
- Frameworks are not to be treated like checklists
- Educate auditors about risk management thinking and their appropriate role
- Instill cybersecurity thinking into the culture of the organization starting with new hire onboarding, regular education and resource distribution, and testing of knowledge

ACTION ITEMS

- [ ] Participate in Cybersecurity Awareness Month
- [ ] Review and update your incident response contact list
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]

NOTES

NOVEMBER/11

1	WED	First Day of American Indian Heritage Month
2	THU	
3	FRI	
4	SAT	
5	SUN	Daylight Saving Time ends
6	MON	
7	TUE	
8	WED	
9	THU	
10	FRI	Veterans Day (substitute)
11	SAT	Veterans Day
12	SUN	
13	MON	
14	TUE	
15	WED	
16	THU	
17	FRI	
18	SAT	
19	SUN	
20	MON	
21	TUE	
22	WED	
23	THU	Thanksgiving Day
24	FRI	
25	SAT	
26	SUN	
27	MON	
28	TUE	
29	WED	
30	THU	

YOUR CHALLENGE

THE 18 CIS CRITICAL SECURITY CONTROLS

With just two months left in the year and the holidays on the horizon, one can't help but stare at the changing colors of the leaves and sink into introspection. If you have more or less completed each month's challenge, it's time to show what you are really made of. Fine-tune your cybersecurity fortress using the **18 Critical Security Controls** (CIS Controls) found in Version 8:

1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets and Software
5. Account Management
6. Access Control Management
7. Continuous Vulnerability Management
8. Audit Log Management
9. Email and Web Browser Protection
10. Malware Defenses
11. Data Recovery
12. Network Infrastructure Management
13. Network Monitoring and Defense
14. Security Awareness and Skills Training
15. Service Provider Management
16. Application Software Security
17. Incident Response Management
18. Penetration Testing

ACTION ITEMS

- [ ] Update or improve your security controls
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]

NOTES

DECEMBER/12

1	FRI	
2	SAT	
3	SUN	
4	MON	
5	TUE	
6	WED	
7	THU	
8	FRI	
9	SAT	
10	SUN	
11	MON	
12	TUE	
13	WED	
14	THU	
15	FRI	
16	SAT	
17	SUN	
18	MON	
19	TUE	
20	WED	
21	THU	
22	FRI	
23	SAT	
24	SUN	Christmas Eve
25	MON	Christmas Day
26	TUE	
27	WED	
28	THU	
29	FRI	
30	SAT	
31	SUN	New Year's Eve

YOUR CHALLENGE

CISA CROSS-SECTOR CYBERSECURITY PERFORMANCE GOALS

If you are responsible for critical infrastructure you have one final challenge left. (If you are not, continue with November's challenge and shop for Christmas gifts.) To accelerate adoption of essential actions to improve cybersecurity across the nation's critical infrastructure providers, the Cross-Sector Cybersecurity Performance Goals (CPGs) recommend an abridged subset of actions to help organizations prioritize their security investments. The memorandum developed by CISA, NIST, and the interagency community created baseline cybersecurity goals that are consistent across all critical infrastructure sectors.

The CPGs supplement the NIST Cybersecurity Framework (See March) for organizations "seeking assistance in prioritizing investment toward a limited number of high-impact security outcomes, whether due to gaps in expertise, resources, or capabilities or to enable focused improvements across suppliers, vendors, business partners, or customers." The core document covers account security, device security, data security, governance and training, vulnerability management, supply chain, third-party risk, and response and recovery.

In late 2022, CISA started working with Sector Risk Management Agencies (SRMAs) to build on this foundation to develop sector-specific goals.

Happy Holidays!

ACTION ITEMS

- [ ] Semiannual update to your playbooks
- [ ] If applicable, review critical infrastructure security performance
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]

NOTES

ABOUT CXO REVOLUTIONARIES

CREATED FOR CXOs BY CXOs

Learn from IT leaders bringing a new wave of cloud- and mobile-first technology to major enterprises globally. The website publishes the latest insights by digital transformation pioneers and thought leaders.

VISIT CXO REVOLUTIONARIES

ABOUT ZSCALER

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest in-line cloud security platform.

Visit Zscaler

SPONSORED BY: zscaler™