WPO SPARK KIT: Cyber Readiness & Resilience

A curated facilitator kit for WPO Chairs and members

How to use this Spark Kit

This kit offers you an easy way to facilitate a group discussion about **Cyber Readiness and Resilience**. To get started, we recommend the following steps:

- Review the recommended reading list in the **Spark Resource Summary** chart below.
- Click through the links to see complete articles in Spark, OR simply read the **Executive Summaries** (starting on page 4) for quick reference. If you don't love reading you can gain some insight by watching the short video linked below.
- Prepare to facilitate your discussion using the prompting questions & tips suggested on pages 2-3.

Topic Outline

Complete cyber protection is a myth. Given the inevitability of breaches and failures, cyber resilience is the new focus. Learn how to develop recovery processes, tools and mindset to ensure you can bounce back effectively from any cyber eventuality.

Spark Resource Summary

The chart below contains a carefully curated selection of Spark content to assist you in learning more about the topic and leading your discussion. You are encouraged to read the complete articles. However, for your convenience, we've also provided **Executive Summaries and Key Points starting on page 4** to simplify your preparation.

Spark resource Summary	Time Commitment
1. Cybersecurity Is Not (Just) a Tech Problem	Video – 3 min watch
2. Your Employees are Your Best Defense Against CyberattacksWhen	Article – 7 min read
3. When Cyberattacks are Inevitable, Focus on Cyber Resilience	Article – 7 mins read
4. Your Biggest Cybersecurity Risks Could be Inside Your Organization	Article – 6 min read
5. Most Companies Can't Handle Cybersecurity Alone	Article – 4 min watch
6. A Tool to Help Boards Measure Cyber Resilience	Article – 9 min read

Women Presidents Organization

WPO SPARK KIT: Cyber Readiness & Resilience

A curated facilitator kit for WPO Chairs and members

Preparation for Spark Discussion

WPO Chairs: Share any portion, or all of this kit with your members ahead of your meeting and encourage them to review the video, articles or summaries.

WPO Members: Feel free to use this kit with your team to generate valuable discussion about the topic. **NOTE:** Your team will not have access to the full articles unless you have a company Spark subscription. But you are welcome to share the article summaries or download PDFs from your own account.

Scope for: Cyber Readiness & Resilience

This Spark kit creates an opportunity for members to share experiences and best practices related to cyber readiness, security and resilience, ideally highlighting areas of vulnerability and helping to get better measures to protect and recover.

Your aim as facilitator is to draw out the wisdom in the room and encourage members to learn from both the successes and failures of their peers.

Potential Learning Opportunities

- The need to make an organizational shift in focus from cyber protection to cyber resilience.
- Simple and affordable ways to reduce chances of cyber breaches.
- The importance of the leader's role in modelling safe cyber behavior and leading recovery practices.
- Resources and options to support effective cyber security and recovery.
- A balanced scorecard approach supporting Board education and meaningful engagement.

If you have gotten this far in the kit, you get a gold star! * *Keep going – so much more learning ahead!*

WPO SPARK KIT: Cyber Readiness & Resilience

A curated facilitator kit for WPO Chairs and members

Spark Materials Learning Discussion (30 – 90 minutes)

If your members successfully read any of the articles or watched the video, we suggest leading a discussion framed by the following questions:

1. What was your most significant learning from the video or articles?
2. What are you planning to do differently as a result of your learning?
3. What challenges do you face in shoring up your cyber security, or developing a more robust recovery plan? And how will you overcome these challenges?

Plan B

In case no one did any of the pre-work (which we know is the most likely scenario), you can still lead a great discussion to learn from the experience of each member.

Member Experience Cyber Discussion (30 – 60 minutes)

Use a round table approach to explore member challenges related to cyber security and recovery. Ask participants to focus on their learnings and outcomes vs detailed story telling.

Encourage each member to share best practices, success stories and resources related to cyber readiness and resilience.

Debrief and Commitment Capture:

This topic will likely create a to-do list for many members. Feel free to use the commitment tracker to make note of member actions so that you can follow-up at a future meeting if that is a practice your members appreciate.

You may also choose to use a flip chart or white-board to capture the input and look for the trends in terms of which strategies are most popular and successful.

Women Presidents Organization

WPO SPARK KIT: Cyber Readiness & Resilience

A curated facilitator kit for WPO Chairs and members

EXECUTIVE SUMMARY & KEY POINTS FOR SPARK RESOURCES

(NOTED IN CHART ON PAGE 1 – READ THESE SUMMARIES OR FIND THE FULL ARTICLES IN SPARK)

Your Employees Are Your Best Defense Against Cyberattacks

EXECUTIVE SUMMARY

Cybercriminals have exploited social engineering techniques to defraud organizations of billions of dollars, impacting productivity and reputations. The human factor is pivotal in most breaches, with attackers leveraging psychological tactics to manipulate individuals. Business leaders must foster a security-aware culture to mitigate these threats. Cialdini's principles of influence can guide strategies to enhance this culture, ensuring employees are committed to security beyond basic training.

KEY POINTS

1. **Sign a Security Policy:**
    a. Employees should voluntarily sign a clear security policy.
    b. Public commitments increase adherence to security standards.
2. **Elicit Reciprocity:**
    a. Leaders can encourage security behaviors by providing employees with tools like encrypted flash drives.
    b. The norm of reciprocity fosters unconscious compliance with security measures.
3. **Leverage Scarcity:**
    a. Emphasize the rarity and value of the organization's security accreditations.
    b. Implement classification systems to highlight the importance of protecting sensitive information.
4. **Be Like Those You Lead:**
    a. Leaders should show empathy and share personal security struggles.

b. Humility and approachability increase employees' willingness to follow security directives.

5. **Leverage the Value of Authority:**

   a. Senior leaders should actively instruct and educate employees on security.

   b. Combining authority with demonstrated expertise is most effective in enforcing security compliance.

By integrating these strategies, leaders can create a robust human firewall, countering cyber threats and fostering a strong security culture within the organization.

When Cyberattacks Are Inevitable, Focus on Cyber Resilience

Executive Summary

Keri Pearlson discusses a prevalent error among cybersecurity experts: focusing solely on preventing cyber-attacks rather than also preparing for inevitable breaches. Given the rapid emergence of new vulnerabilities and advanced attack vectors, complete protection is unattainable. Pearlson advocates for a shift from a prevention mindset to a resilience mindset, which involves preparing for, responding to, and recovering from cyber incidents. This approach ensures minimal damage from breaches and faster recovery. She outlines practices of resilient organizations, such as fostering a culture of cybersecurity, conducting regular response drills, adopting secure-by-design principles, and having robust communication plans.

Key Points

1. **Current Cybersecurity Focus:**

   a. Experts often prioritize preventing breaches over preparing for them.

   b. Complete protection is impossible due to constant new vulnerabilities.

WPO SPARK KIT: Cyber Readiness & Resilience

A curated facilitator kit for WPO Chairs and members

2. **Need for Cyber Resilience:**
    a. Cyber resilience involves preparing for, responding to, and recovering from cyber incidents.
    b. A resilience mindset complements prevention with robust recovery plans.
    c. Cyber resilience is about minimizing harm and maximizing recovery post-incident.
    d. Many organizations currently focus more on prevention than on resilience.
3. **Framework and Practices:**
    a. The NIST Cybersecurity Framework emphasizes protection and resilience.
    b. However, companies tend to prioritize protection components over resilience.
4. **Challenges with Current Approaches:**
    a. Prevention is easier to justify and quantify, while resilience has a softer ROI.
    b. Defense remains vital but insufficient alone.
5. **Traits of Resilient Organizations:**
    a. **Culture of Cybersecurity:** Involves everyone from employees to the board.
    b. **Preparedness and Practice:** Regular exercises to simulate and respond to incidents.
    c. **Secure by Design**: Incorporating security into the organizational and technological design from the start.
    d. **Robust Communication Plans:** Ensuring effective communication even when primary systems are compromised.

WPO SPARK KIT: Cyber Readiness & Resilience

A curated facilitator kit for WPO Chairs and members

Your Biggest Cybersecurity Risks Could Be Inside Your Organization

Executive Summary

As digital threats grow in complexity and volume, organizations must prioritize managing both external and internal risks, with insider threats posing significant challenges. Effective insider risk management hinges on balancing employee trust, collaboration across functions, and advanced detection tools. By fostering a trust-based culture, empowering employees through education, and utilizing machine learning tools, companies can mitigate insider threats while maintaining productivity and privacy.

Key Points

1. **Prioritize Employee Trust and Privacy:**
    a. Trust is fundamental in insider risk programs.
    b. Implement privacy controls and policies that protect employee privacy.
    c. Use role-based access to ensure appropriate handling of compliance alerts.
    d. Transparency and narrowly defined scopes in investigations build trust.
2. **Collaborate Across Functions:**
    a. Insider risk is a business-wide issue, not just for IT and security.
    b. Engage legal, HR, and senior leadership for wider buy-in and diverse perspectives.
    c. Establish a response plan detailing roles, responsibilities, and shared goals.
    d. Quantify metrics to fine-tune the process and reduce false positives.
3. **Recognize Employees as the First and Last Line of Defense:**
    a. Regular training on data protection and compliance is crucial.

b. Emphasize the importance of data stewardship and personal data protection.

c. Foster a culture of "see something, say something" in a risk-free manner.

4. **Use Machine Learning Tools to Do More with Less:**

a. Modern tools detect and mitigate risks with adaptive security capabilities.

b. Machine learning identifies subtle patterns indicating insider threats.

c. Advanced tools reduce false positives, enhancing productivity.

d. Integrated tools balance security needs with user privacy.

Balancing people, processes, and technology is key to managing insider risks effectively. Trust, transparency, and collaboration are essential in building a proactive and continuous risk management strategy. This approach, supported by powerful technology and a healthy work environment, is crucial for preventing, detecting, and responding to insider threats efficiently.

Most Companies Can't Handle Cybersecurity Alone

EXECUTIVE SUMMARY

Cybersecurity is becoming increasingly difficult for organizations to manage on their own due to the rapid evolution and complexity of cyber threats. Despite investments in technology and personnel, many organizations remain vulnerable. Cybersecurity-as-a-service (CSaaS) offers a viable economic solution, providing access to specialized security operations professionals and advanced tools. This approach not only reduces the risk of debilitating cyberattacks but also enhances the effectiveness of existing security investments, optimizes cyber insurance positions, and allows internal teams to focus on strategic initiatives.

WPO SPARK KIT: Cyber Readiness & Resilience

A curated facilitator kit for WPO Chairs and members

KEY POINTS

1. **High Cost of Inaction:**
    a. The average cost to remediate a ransomware attack for small or mid-sized organizations is $1.82 million.
    b. Cyber incidents can lead to significant business losses, as seen with this articles example of Royal Mail's six-week disruption due to a ransomware attack.
    c. Cyber insurance may cover some costs but cannot mitigate all commercial impacts.
2. **Technology Alone is Insufficient:**
    a. Essential cybersecurity technologies need to be complemented by 24/7 monitoring and incident investigation.
    b. Human experts are necessary to fully assess and neutralize threats.
    c. Without professional security operations, organizations risk greater exposure and fail to maximize their security investments.
3. **Need for Specialist Operators:**
    a. Effective detection and neutralization of threats require constant monitoring by skilled security professionals.
    b. Many organizations lack the necessary tools, personnel, and processes in-house.
    c. Workforce shortages exacerbate the challenge, increasing the need for external cybersecurity resources.
4. **Benefits of CSaaS:**
    a. **Risk Mitigation:** Lower risk of severe cyberattacks at a fraction of the recovery cost.

b. **Cost Efficiency:** Outsourced services offer expertise and responsiveness that are difficult and expensive to maintain in-house.

c. **Strategic Focus:** Frees up internal teams to focus on strategic business initiatives.

d. **Enhanced Investments:** Makes better use of existing security tools to improve overall defenses.

e. **Cyber Insurance Optimization:** Meets high security standards required by insurers, improving policy terms and reducing the likelihood of claims.

5. **Economic Imperative:**

a. Prioritizing cybersecurity is crucial for operational stability and financial health.

b. CSaaS provides a practical and economically sound solution for managing cybersecurity in today's fast-evolving threat landscape.

A Tool to Help Boards Measure Cyber Resilience

EXECUTIVE SUMMARY

This article is best to read in its entirety in order to appreciate some visual examples of a Balanced Scorecard for Cyber Resilience.

Boards of directors must shift their focus from cyber protection to cyber resilience to effectively mitigate cybersecurity risks. Traditional metrics and technical details are often inadequate for ensuring resilience. A new approach, using a balanced scorecard, offers a comprehensive framework combining financial, technological, organizational, and supply-chain indicators. This framework helps boards understand the business risks and enables productive dialogue between directors and cybersecurity leaders. Boards need both qualitative and quantitative assessments to ensure their organizations can continue operating amidst cyber threats.

WPO SPARK KIT: Cyber Readiness & Resilience

A curated facilitator kit for WPO Chairs and members

KEY POINTS

1. **Shift from Protection to Resilience:**
    a. Boards must prioritize discussions on cyber resilience over cyber protection.
    b. Protecting assets, systems, and data is important, but not sufficient.
    c. Focus should be on plans to respond and recover quickly from cyberattacks.
2. **Board Oversight and Information Needs:**
    a. Boards need relevant information to oversee cyber risk effectively.
    b. Traditional metrics (e.g., phishing exercise results) are inadequate for board-level discussions.
    c. A balanced scorecard approach provides business-relevant indicators of cyber resilience.
3. **Balanced Scorecard for Cyber Resilience (BSCR):**
    a. Combines financial, technological, organizational, and supply-chain indicators.
    b. Includes three components: biggest risk, action plan, and overall indicator (green, yellow, red) for quick risk assessment.
    c. Helps boards understand and discuss the real business risks and resilience strategies.
4. **Research Findings on Board Reporting:**
    a. Cybersecurity leaders report technical metrics that do not help boards ensure cyber resilience.
    b. Boards need information about system assets, proactive capabilities, and recovery speed.

c. Financial impact, third-party risk assessments, and supply-chain security are critical areas of interest.

5. **Challenges and Recommendations:**
   a. Boards struggle to discuss cybersecurity at a meaningful level.
   b. Directors want comparisons and insights into peer practices and resilience.
   c. A mindset change is needed from protection metrics to resilience assessments.
6. **Implementing the Balanced Scorecard:**
   a. Provides a comprehensive view of cyber risks and resilience.
   b. Facilitates productive conversations between boards and operational leaders.
   c. Ensures business preparedness for potential cyber disruptions.
7. **Next Steps for Boards and Cybersecurity Leaders:**
   a. Shift focus from protection measures to resilience strategies.
   b. Provide qualitative and quantitative assessments of business impact from cyber risks.
   c. Ensure discussions cover broad organizational vulnerabilities, not just specific threats like phishing.

By adopting a balanced scorecard for cyber resilience, boards can better understand and manage the dynamic nature of cyber risks, ensuring their organizations remain resilient and operational even in the face of cyber incidents.

Women Presidents Organization

WPO SPARK KIT: Cyber Readiness & Resilience

A curated facilitator kit for WPO Chairs and members

Capturing Commitments & Key Learnings

Who	Commitment / Action	Insights / Learning
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		

WPO SPARK KIT: Cyber Readiness & Resilience

A curated facilitator kit for WPO Chairs and members

How to Access and Use Spark

Q: How do I log in to access HMM Spark?

A: The HMM Spark login page can be accessed online **HERE**. You can also access it from the WPO Homepage: www.women-presidents.com > Login (top right) > Login under Spark.

Q: What is my username and password?

A: Your username will be the email you have on file with the WPO. You will be prompted to create your own password prior to logging in for the first time.

d. Please select the "Forgot Password" link under the HMM Spark portal login.

e. Enter your email, and the system will prompt you to create a password.

f. Once you have created a password, you may log in using your email address and newly created password.

Q: I am being prompted with "What skills would you like to develop?" Are my skill selections permanent?

A: After the initial account setup, you **must** select at least one skill in order to receive personalized learning pathways and full access to the HMM Spark portal. Please note that the skill selections can be updated at any time by going to **Your Profile > Skills**.

Q: I forgot my password. What are the steps to reset my password?

A: To reset your password, please select the "Forgot Password" link under the HMM Spark portal login.

Q: Am I able to adjust the frequency at which I receive emails from HMM Spark?

A: Yes! Each member is automatically set up to receive a daily digest email with information that is relevant to their interests (based on their initial selections). Members can adjust the frequency of the digest emails at any time by going to **Profile Settings > Communications**.

If you are still having issues, be sure to reach out to Tomi Jane.