The 4P's to Combatting Cyber Risk
A Quick Reference Guide

Planning

Conduct a comprehensive inventory

- Can you track all transfers and storage of company assets and data, including back-up?
- What are your regulatory requirements for protection and transmission of data? What are your current measures in place for complying and keeping data protected?
- Where do your systems and applications "live" on your network?

Identify your Incident Response Plan

- What components of a risk event or breach are you obligated to report, and to whom?
- What is the implementation process flow, including mitigation, restoration, and reporting details?
- Is your plan tested?

Understand your cyber policy

- What does your liability insurance coverage cover in cyber incident scenarios? Are there exceptions?
- What resources are available to enhance your understanding of the role your policy could play?

Know your vendor contracts

- In reviewing your vendor agreements, you should pay particular attention to the following critical contract provisions:

  1) Limitation of Liability: Most vendor contracts include a limitation of liability provision that limits a vendor's liability. Review the limitation of liability provision in your vendor agreements to ensure that you have the appropriate amount of coverage for damages that flow from a vendor-caused cyber risk liability event.

  2) Consequential Damages: Most vendor contracts preclude the ability to recover consequential damages that would likely flow from a cyber risk liability event. Review the indemnification provision in your vendor agreements to ensure that you have the ability to recover the types of damages that are likely to flow from a vendor-caused cyber risk liability event.

  3) Indemnification: Your vendor agreements should include an indemnification provision through which your vendor is obligated to indemnify you for third-party claims that result from a vendor-caused cyber risk liability event.

Protection

Access controls

- Do your employees only have access to the tools and data required for them to do their jobs?
- Do only system administrators have administrative-level privileges?
- Do you have multi-factor authentication in place?
- What are your password policies and requirements?
- What are your policies for remote network access? Is there a VPN available to secure data?

Multi-layered security and patching

- What is your method for ensuring that all systems and software are fully up-to-date?
- How often are your auditing your network for possible vulnerabilities in order to patch those?
- What are your current cyber security tools, and how to they work? What are the layers?
- How do you test your own network to identify potential weaknesses?
- What is your data backup plan, how does it work, and who has access to the backups?

(continued on next page)

Strong contracts, policies, and procedures

- What are your acceptable use policies for your resources?
- What are your enforcement mechanisms?
- Do these tools align with industry and regulation requirements?
- How do you require employees to dispose of sensitive information and materials appropriately?
- What are your vendors' security policies and procedures that may affect you and your data?

Create a culture of security

- Have you communicated the significance of cybersecurity to the business's overall success?
- Are your employees trained to avoid cyber threats and identify possible breach and risk scenarios?
- Are those responsible for assets and tools confident that your tools are current and best-in-class?

Precaution

Train and test your team

- Your employees are your weakest link. Traditional threat defenses play their part, but addressing employee behavior with security awareness training and simulated cyber attacks could prove critical to your overall security posture as an organization.

Communication with key players

- Who is involved in your incident response plan, and when does each come into play?
- What are your external support resources and where is that contact information stored?
- How available will your resources be in case of an event? If unavailable, what are alternatives?

Augment your policies

- Are there gaps in your cyber liability policy? See counsel.
- Does your business require supplements due to certain added regulations or risks apparent?
- Are you getting the best "bang for your buck" given your needs and requirements?

Negotiate your contracts

- Engage an attorney immediately to audit your contracts and subsequently hold vendors accountable.
- Ensure that internal cyber event-responsive communications are protected by an attorney-client privilege in advance of any cyber risk event to avoid reporting complications.

Prevention

Security vigilance

- Ensure consistent proper handling of sensitive information (PII, PHI, PCI-DSS, IP) across channels.
- Implement testing and measure the progress of your tools and training.
- Encourage customers, too, to flag suspicious behavior with communications and transactions.

Proactive solutions

- Avoid firefighting by detecting and mitigating threats and risk scenarios prior to security events.
- Find tools that are right for your business model and industry.
- Lean on business partners and resources to build robust policies, procedures, and contracts.

Documentation

- All methods and techniques employed to address potential risks must be recorded. Detail required is highly contingent on policies, contracts, and regulatory requirements.
- Maintain a current inventory of all network components and data.
- Keep legal and insurance resources up-to-date on vendors and tools, as they may affect coverage.

Keep your tools and resources current

- Next-gen tools and approaches are necessary to maintain the ability to combat current relevant risks. The threats landscape is perpetually evolving, and your resources should stay ahead!