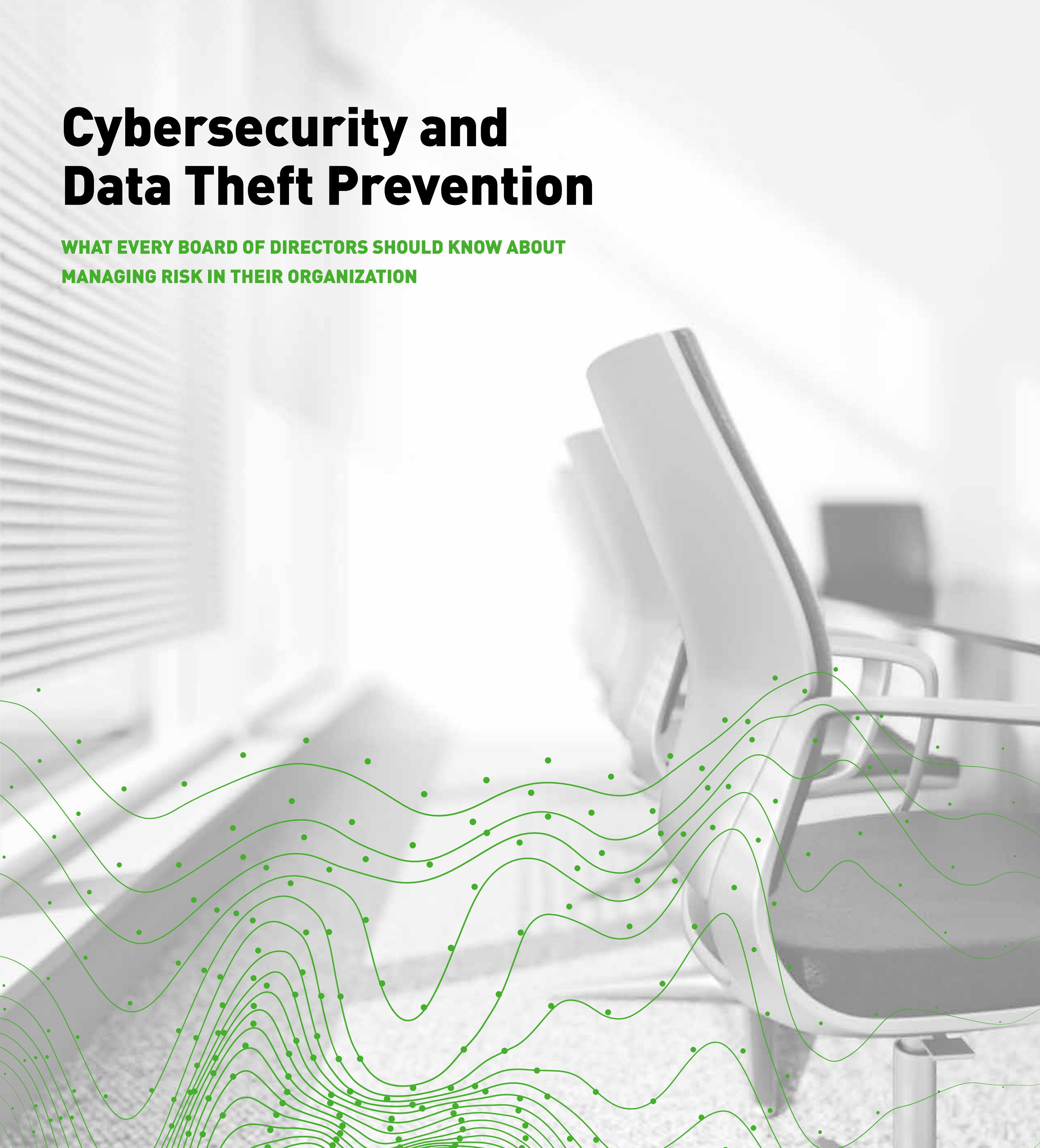
FORCEPOINT
POWERED BY Raytheon

Whitepaper

Cybersecurity and Data Theft Prevention

WHAT EVERY BOARD OF DIRECTORS SHOULD KNOW ABOUT MANAGING RISK IN THEIR ORGANIZATION



Scope of this Document

The primary responsibility of any board of directors is to secure the future of the organization(s) they oversee. To do so, board members need consistent access to information on circumstances and risks that could affect the future of the organization. Cybersecurity is a prime example of information that directly affects the wealth and future prospects of an organization but has heretofore not been subject to board level review and oversight.

However, in the wake of the devastating number of high-profile cyber incidents and their significant financial and legal ramifications, cybersecurity is no longer a topic that can be left solely to the IT department. It is now essential that the board ask strategic and thoughtful questions on how well the organization they oversee is prepared to face the new world of high-risk data breaches and realize continued success in these tumultuous times.

This document provides a non-technical overview on cybersecurity and provides recommendations for the topics that every board member should consider.

LEGAL NOTICE

Please note that this document represents the views and interpretations of the authors and editors, acting on behalf of Forcepoint™, unless stated otherwise. This publication should not be construed as legal advice from Forcepoint. Third-party sources are quoted as appropriate. Forcepoint is not responsible for the content of the external sources, including external websites referenced in this document. This document is intended for information purposes only. Reproduction is authorized provided the source is acknowledged.

Table of Contents

Executive Summary

CYBERSECURITY BECOMES A TOP-TIER ISSUE

2014 saw some of the biggest organizations in the world became victims of costly cyberattacks and data theft incidents. These high-profile events ushered in a new era for all organizations in which cyberattacks are now a part of doing business. As a result, cybersecurity has become a top-tier issue for all boards of directors. It is, however, a complex and fluid discipline that is beyond most directors' area of expertise. This document will guide directors in their approach and assessment of the cybersecurity posture and processes of the organization(s) they oversee.

FIVE TENETS OF CYBERSECURITY OVERSIGHT FOR THE BOARD OF DIRECTORS

Forcepoint identifies five tenets that provide directors the foundation to accomplish the formidable-but-necessary task of cybersecurity oversight at the board level:

- Tenet 1: **Cybersecurity is a risk management issue, not a technological one.**

  The board of directors must demand a regular health check and risk assessment of the organization's security posture.

- Tenet 2: **Provide meaning behind the metrics – make cybersecurity real to the board.**

  The board must be briefed by the Chief Information Security or Chief Risk Officer at every meeting. These roles should report directly to the board.

- Tenet 3: **Board members must understand the legal aspects of cybersecurity regulations.**

  A data breach exposes organizations to the risk of civil and criminal disciplinary actions and fines by regulatory bodies, class action suits from customers and shareholders as well as legal actions by affected partners.

- Tenet 4: **Board members must identify acceptable risk levels in business operations.**

  Business judgment applies to cybersecurity as a part of business operations. Boards must quantify and manage cybersecurity risk as they do in other business categories.

- Tenet 5: **Board members must adopt a well-defined risk management framework.**

  The framework is a risk-based compilation of guidelines designed to help assess current capabilities and the creation of a prioritized plan for improving cybersecurity practices.

Key Areas of Inquiry for the Board

For effective oversight, directors will need to identify:

1. The organization's critical data.
2. Current risks to that data.
3. Key performance indicators of the security posture.
4. Data breach protocol for mitigation, remediation and public relations.
5. Procedures for upgrading the security posture and training personnel.

Cybersecurity and Data Theft Prevention: What Every Board of Directors Should Know about Managing Risk in their Organization

KEY TENETS FOR THE BOARD

With 22,000 customers worldwide, Forcepoint has an established track record developed over more than 20 years of experience as a leading cybersecurity provider. During this significant period of time, Forcepoint has developed a series of cybersecurity tenets which can serve as the strategic foundation for a board of directors' approach to understanding the tools and processes of an effective cybersecurity posture.

Tenet 1: Cybersecurity is a risk management issue, not a technological one.

Sophisticated organizations look at cybersecurity through the prism of risk management. At the board level, business risks are categorized into one or more of the following:

- Business disruption risk.
- Reputational risk.
- Legal risk.
- Regulatory and compliance risk.

Cybersecurity risk will fall under one or more of these categories, depending upon the organization's business model and sensitivity to various types of risk.

The board of directors must receive and review an update and business risk assessment of the organization's security posture at every board meeting. The board will need to prioritize the elements of every cybersecurity risk assessment as each applies to its respective business risk. By asking the questions below, boards can ensure they have a proper understanding and context of cyber risks to the organization:

1. Have we identified the value of the organization's most critical information assets?
   - What information makes the organization competitive?
   - What percentage of the overall information assets does this represent, and where is it stored, used and shared?

2. Have we received a detailed summary on the security incidents that have occurred (including those attacks that were successfully thwarted)?
   - What intelligence can be gained from these threats and attacks?
   - How can that intelligence be most effectively applied for incidence remediation and prevention of future attacks?

3. What assurances do you have that employees, suppliers, partners, overseas subsidiaries, cloud providers, etc., can be trusted with the organization's most critical information assets?
   - What controls are in place to militate against anticipated risks and how well documented are these?

4. What is the appetite for risk in the organization?
   - How well documented is this?
   - How is this risk posture reflected in operations and decision making?

5. To what extent are the representatives across the business, e.g., Manufacturing, Operations, R&D, Legal, HR, etc., engaged in an organization-wide and regular risk-based discussion on cybersecurity?

6. Has the business quantified the potential business effects of cyberattacks – i.e. data loss, disruption and costs arising from a failure to protect the organization from a significant incident?

7. Has the organization benchmarked its risk posture and integrity against comparable organizations that may be open to this form of information sharing?

8. Has the organization tested its cyber resilience and response in the wake of a significant incident? Has this testing been incorporated into the organization's disaster recovery and business continuity planning process?

9. Does the person responsible for cybersecurity have a mentor among the board members to help them prepare information in the most appropriate manner possible?

Tenet 2: Provide meaning behind the metrics – make cybersecurity real to the board.

Every board meeting should discuss the topic of cybersecurity to some degree. Board members are generally tired of hearing about threats. Instead, they want to hear about risks and understand the impact of what the organization has witnessed. Avoid repeating meaningless KPI statistics that hide the true nature of what is happing in the organization's infrastructure. At its core, the board wants to know "How secure are we?"

The Chief Information Security or Chief Risk Officer should report directly to the board. They should not be "buried" within the IT or Operations departments. The board of directors must probe the officer in charge of cybersecurity to do the following:

1. Focus on metrics that explain the impact attacks have or could have had on the organization. How have these metrics changed since the last review period and what might one infer from such changes?

2. Report by department who has been targeted and the nature of the attack. Indicate how well the organization's security mechanisms responded and quantify, if possible, the impact of a successful attack.

3. Identify the overall cybersecurity strategy and response to known risks and attempted attacks.

4. Explain the key issues that are at the forefront of the officer's mind.

5. Provide a recap of key incidents that have occurred in the organization's industry and how they relate to the risk-posture of the organization and discuss any roadblocks to implementing a holistic Data Theft Prevention approach. This is a key metric, as it is relevant to the board in terms of legal risk. The board must have a clear understanding of how well the organization is protected, organized and prepared in its security posture relative to its industry peers. If an industry peer suffers a data breach and the board's organization is similarly protected, the board will know that a higher level of security is needed. Meeting or surpassing industry security standards may also help the organization avoid punitive damages should it fall victim to data theft. On the other hand, if the organization's security budget is significantly higher than its peers, it may indicate to the board that they're spending too much money on cybersecurity, the security resources are inefficiently allocated, or both.

The board must also, from time to time, seek external review of the cybersecurity in place to gain an alternative perspective on the organization's risk posture.

Tenet 3: Board members must understand the legal aspects of cybersecurity regulations.

The loss or theft of critical information exposes organizations to the risk of action by regulatory bodies. Moreover, when cyberattacks disrupt business operations, organizations may fail to meet obligations to customers, resulting in class-action suits from customers and even shareholders.

Furthermore, the U.S. Securities and Exchange Commission has stated that "Public companies that are victims of cyber-attacks should consider disclosing additional information beyond what's required to help protect customers whose private data could be at risk." Also, knowledge of a cyberattack may be regarded as information likely to inform investment decisions and be treated as "inside information" that meets the "reasonable investor" test.

There are three broad areas of concern with regards to legal frameworks:

1. **Compliance with national and industry-specific regulations** – Personally-identifiable information (PII) and other data present huge privacy and compliance risks for organizations. Compliance is complex and multi-layered, with national and industry-specific security and privacy laws often varying widely. Directors must ensure that management is aware of civil and criminal liabilities that may attach to failure to comply with security and privacy compliance schemes. Many organizations have at least some level of program in place to manage cyber risk. Such risk programs should be incorporated within overall corporate risk management strategies with the appropriate executive control and authority.

2. **Risks and liabilities associated with third-party service providers** – Directors should probe the contractual relationships and liabilities with IT outsourcing, business process outsourcing and cloud computing providers. Many third-party agreements are vague on the definitions of who is responsible for the safeguarding of the organization's critical information. Moreover, incident notification and remediation procedures are often overlooked. Individuals in the organization have frequently created chains of trust between organizational stakeholders and it is the responsibility of the directors to ensure that such agreements are appropriately defined and audited. Additionally, directors should be aware of what their own organization's security, privacy and reporting obligations are to its customers and partners. Failure to account for this risk could lead to lengthy legal battles and loss of reputation.

3. **Data breach awareness policy and notification processes** – The board must be made aware of major data breaches and has a duty to remain informed of such matters. This duty also pertains to attempted breaches, although there is reasonable latitude allowed with regard to the scale, severity and potential impact of

the breach or attempted breach. Notification processes, however, are complex areas of concern. In the event of a breach – even without the subsequent transmission of the data elsewhere – the board's first priority must be to seek external legal and data breach notification advice in order to establish the correct notification processes in a timely matter.

From the board's perspective, the following information must be recorded for any possible breach declaration:

- The geographic sphere of operations where the information was used and affected. Also very important in data breach notification is the locale of the citizens whose data was impacted. Disclosure laws generally follow the citizen's domicile, not the physical location of the breach itself.

- The reporting requirements in relation to the laws of the specific location - i.e. the legal reporting requirements in Europe differ widely from those in the U.S., for example, and will even vary from state to state within the U.S.

- And, whether or when a breach has occurred is a complex question. Safe harbor clauses may come into effect.

Tenet 4: Board members must identify acceptable cyber risk levels in business operations.

It's important to note that the board of directors always sets the tone for the organization, and as such, communicates to members of the organization how cybersecurity should be viewed. This will have a marked effect on the security culture within the organization. Certainly board members face remarkable challenges, not least is the fact that many may have spent the majority of their careers in the pre-digital era. They must not be fazed by the highly technical jargon used by "experts in the field" or the complexity and fluidity of modern technology. Instead, they must elevate the discussion to one of risk-versus-reward. As a former chief of the SEC's Office of Internet Enforcement recently remarked:

"I do not believe it's realistic to expect board members to have anything but a high-level understanding of the nature of cyber threats and how they impact the business of the corporation. Just as you need a good accounting firm to give you financial expertise, from the board's perspective this field … requires you to tap into … the necessary expertise and make sure your company is doing all it can to protect itself."

However, it behooves all board of directors to educate themselves broadly on the types of cyber risks to which their organization and sector may be vulnerable. As such, directors should request and expect regular updates from the organization on recent trends in industry-specific data breaches and on security intelligence reports from information sharing centers.

In general terms, common sense and business judgment must apply in cybersecurity as much as any other sphere of business operations. Many of the same types of questions and approaches used by boards to quantify and manage other categories of risk, such as insurance and recovery plans, apply equally here as well.

Tenet 5: Board of Directors must adopt a well-defined cyber risk management framework.

The organization should structure its cybersecurity defenses in order that their effectiveness and applicability can be independently assessed. The framework should seek to:

1. Define a set of activities to anticipate and defend against cyber-attacks.

2. Define a set of measurements to assess to what degree an organization has implemented its defense strategies and benchmark how prepared they are to protect systems against an attack.

3. Define a benchmark profile that can be used to identify opportunities for improving an organization's cybersecurity posture by comparing a current profile with a target profile.

One such framework was created by the National Institute of Standards and Technology (NIST). The "Framework for Improving Critical Infrastructure Cybersecurity" was the result of an executive order issued by the U.S. President in 2013 to establish a set of voluntary cybersecurity standards for critical infrastructure companies. The framework is a risk-based compilation of guidelines designed to help organizations assess current capabilities and draft a prioritized roadmap toward improved cybersecurity practices. The NIST Framework also creates a common language for the discussion of cybersecurity issues that can facilitate internal and external collaboration.

There are many other benefits associated with adopting such a framework. First, the NIST Framework may set cybersecurity standards for future legal rulings. Second, organizations that adopt the NIST Framework at the highest possible risk-tolerance level may be better positioned to comply with future cybersecurity and privacy regulations.

It's important to note, however, that there is no one-size-fits-all solution for cybersecurity. The U.S. government cannot provide comprehensive, prescriptive guidelines across all industries. It is therefore the responsibility of the directors to ensure that any framework adopted is appropriate to the circumstances in which it is applied. With that said, there are a number of questions directors should pose to their management teams to begin the process of understanding and managing risk.

KEY AREAS OF INQUIRY FOR THE BOARD

Having established the broad tenets of a comprehensive cybersecurity strategy, the following is a list of areas that directors may wish to refer to in their next board meeting:

1. **Identify the organization's critical data.**
   - What is our most critical data that drives the business success?
   - Where is it stored, used and shared?
   - What are the consequences of a breach featuring this information?

2. **Current risks to that data.**
   - What are the top risks facing the organization with regards to cybersecurity integrity when adopting new technology – i.e. new technology such as cloud computing and mobile (BYOD)?
   - What are the third-party risks such as outsourcing and SaaS, and risk of data theft from external actors and Insider Threats?

3. **Key performance indicators of the security posture.**
   - How do we educate employees to raise their Security IQ and create awareness of threats and risky behavior?
   - Do we use independent third parties to periodically test our defenses?
   - What other risk assessment methods have been put in place and what did the results indicate?

4. **Data breach protocol for mitigation, remediation and public relations.**
   - What steps have been taken to manage cybersecurity governance and the legal frameworks for the territories in which the organization operates and the domiciles of individuals from which data is collected?
   - In the event of a serious breach, what protocols and procedures have been developed? Have these been tested?
   - What is the communications plan for the event of a serious information breach?
   - What is the crisis management plan and has it ever been tested?

5. **Procedures for upgrading the security posture and training personnel.**
   - To what extent have we measured the risk of data loss or attack across our extended value chain of partners, suppliers and customers?
   - When was the last major breach? What happened as a result and what lessons were learned?

CONCLUSION

The familiar maxim, "National defense is too important to leave to the military," also applies to the cybersecurity of your organization. Of course, the IT team is on the front lines of cyber defense and monitoring the risk to your data, as it should be; but the impact of data theft is too important for the board of directors not to be involved at a strategic level. For most boards of directors, however, the prospect of overseeing cybersecurity is a formidable task. However, it is certainly achievable with a holistic approach and the right cybersecurity partner.

Forcepoint's Data Theft Prevention solution is an advanced and holistic approach to data security and cyber risk management. It identifies the critical data at the heart of your organization, provides in-depth risk assessment and analysis of your security posture, and prevents your critical data from leaving when it should not. It also enables your organization to innovate and grow with confidence.

These factors and security attributes are the key advantages in performing successful, board–level oversight duties as well as frontline IT security decision-making. Identifying the weaknesses in your security posture, as well as potential threats to your critical data, are the first steps to take when reviewing and assessing your current risk levels. The results of a complete risk assessment will drive the security processes and strategies going forward.

Contact Forcepoint for a complimentary risk assessment of your current security posture with our RiskVision™ technology. It will identify threats that your current system is missing or cannot recognize and then provide you with an in-depth report on your cybersecurity system's weaknesses and vulnerabilities. No security posture, regardless of the investment level, can protect your critical data against threats it cannot see.

To access the latest Forcepoint security insights and connect through social media, please visit www.forcepoint.com/smc.

Recommended Reading & References

1. Framework for Improving Critical Infrastructure Cybersecurity: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
2. The UK Cyber Security Strategy: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
3. The 2015 Forcepoint Threat Report: http://www.forcepoint.com/content/forcepoint-2015-threat-report.aspx
4. 2014 Ponemon Report on CyberSecurity: http://www.forcepoint.com/content/2014-ponemon-report-part-2-thank-you.aspx
5. ENISA's work on National Cyber Security Strategies: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss
6. Related Forcepoint publications on Data Theft Prevention: http://www.forcepoint.com/content/data-theft-prevention.aspx

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT