CyberSheath Annual Security Report

www.cybersheath.com

CyberSheath's Security Forecast Report for 2015

Top 10 Security Forecasts for 2015 and Beyond

CYBERSHEATH
SERVICES INTERNATIONAL, LLC

CyberSheath Legal Disclaimer

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise.

CyberSheath reserves the right to modify the contents of this document at any time without prior notice. Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although CyberSheath uses reasonable efforts to include accurate and up-to-date information herein, CyberSheath makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. CyberSheath disclaims all warranties of any kind, express or implied. Neither CyberSheath nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

10	Compliance Mandate for Cyber Security Intelligence Sharing
9	Vulnerability Management Surges in Criticality
8	Mobile Security Becomes a Top Priority
7	Privileged Misuse Incidents Shift to the Front Lines
6	NIST Cybersecurity Framework Gains Even More Traction
5	Third Parties Become an Enterprise Risk Management Focus
4	Increased Dependency on Outsourced Security
3	Security Moves to Big Data and Bleeding Edge Technology
2	Enterprises Develop Response Plans for Ransomware
1	Boards Demand Greater Accountability from Security Teams

Executive Summary

The past 12 months have seen extraordinary levels of threat actor activity. High profile data breaches, like those at Target, Staples, and most recently, Sony Pictures Entertainment, have dominated the newsroom floor and occupied boardroom conversations. Cybersecurity in 2015 will be on the to-do list of every major organization with intellectual property, personally identifiable information, medical information, and critical infrastructure to protect.

Looking forward to 2015, the proceeding security trend forecasts capitalize on issues and activities that need to come to light in order for a security team to function efficiently in today's threat landscape. The next 12 months in 2015 will shine a spotlight on security offices for public and private organizations around the world as new threats emerge.

In the coming months, we expect an increase in intelligence sharing among public and private corporations to better understand our digital adversaries in an effort to prevent massive and potentially embarrassing data breaches. Organizations will increasingly rely on vulnerability management programs to help shift security teams to take a proactive approach, rather than reacting to a breach. While other trends will peak in 2015, from mobile security to increased use of the NIST Cybersecurity framework, it is the board of directors for companies, leadership teams and CEOs that will demand more accountability from their cybersecurity teams in the face of continuous streams of threats.

CyberSheath, a leading provider in professional security services, manages information about thousands of attacks on enterprises giving us a unique perspective on emerging trends in cyber security. Our security research team is happy to share the summary of emerging trends for 2015.

10. Compliance Mandate for Cyber Security Intelligence Sharing

Cyber security has gained significant public mindshare and a greater focus in 2014. The threat intelligence market is growing and evolving rapidly and Gartner predicts that by 2019, 60% of security organizations will rely on threat intelligence feeds as a functional requirement to ensure their operational resiliency. Data illustrates that integrated security intelligence makes other security monitoring and controls far more effective. In 2015, we forecast that public and private cyber security intelligence sharing will become mandatory for enterprises through updated compliance regulations for defense, payment, healthcare, and financial industries.

9. Vulnerability Management Surges in Criticality

We saw major vulnerabilities events in 2014 with the open source vulnerabilities Heartbleed and Shellshock and the critical infrastructure attacks with the Stuxnet worm. These large scale events all point back to a systemic problem the industry faces with ineffective vulnerability management programs as the majority of large scale events could have been remediated significantly faster with a robust vulnerability management program. In 2015, we will see a continued trend in data breaches through well-known vulnerabilities as a result of weak strategic security investments that drive ineffective vulnerability management programs driving the demand for businesses to invest in their vulnerability management programs in order to successfully identify critical vulnerabilities and create a repeatable plan to first remediate critical vulnerabilities.

8. Mobile Security Becomes a Top Priority

Mobile technologies, such as tablets and smart phones, are taking an increasing share of the internet usage and attackers are shifting accordingly at an alarming pace. Android with its quickly growing market share will take the lion-share of attacks but iOS platforms, such as iPhone and the iPad (although much more difficult to attack), will continue to see new malware. In 2015, we forecast that companies will be forced to seriously reconsider their mobile security strategy and define a technological solution and a roadmap that keeps company data safe by protecting corporate liable devices from malware, spyware, and those that are lost or stolen.

7. Privileged Misuse Incidents Shift to the Front Lines

Last year we saw 80% of all known cyber incidents connect back to privilege misuse. Businesses typically perceive privileged account exploitation as the last line of defense before a data breach as this means the attackers gain dangerous levels of access to critical IT infrastructure. In 2015, we forecast that attackers will continue to target privileged access and businesses will need to procure privileged identity management tools, such as those from CyberArk, to detect critical attacker intrusions and movements and prevent their crown jewels from being stolen.

6. NIST Cybersecurity Framework Gains Even More Traction

Last year we witnessed major cyber security breaches with Target, Home Depot, Staples, and recently Sony Picture Entertainment. These events underscored the need and the importance of good cybersecurity practices to rapidly detect cyber intrusions and promote security resilience across an enterprise. In 2015, we forecast that businesses will heed the advice from the leading industry security experts and the White House Administration to seek out and employ the NIST Cybersecurity framework's best practices to assess their IT infrastructure and limit their risk exposure to protect against the modern cyber threats businesses face today.

5. Third Parties Become an Enterprise Risk Management Focus

Last year the volume of outsourced products and services have surged alongside their associated security risks. This is best captured by the risk business consulting firm Protiviti, they stated "Despite this, for most organizations, understanding vendor risk and how to manage it appropriately has thus far been more art than science". In 2015, we forecast that businesses will have to invest seriously in third party risk management tools, such as RSA Archer, to manage the large volumes of third-party relationships and streamline risk-based vendor selection, relationship management, and compliance monitoring as part of the business next generation GRC program.

4. Increased Dependency on Outsourced Security

Investing in security technology is a vital part of any businesses overall security program. Challenges, however, can arise once these products arrive and are ready to be deployed within the network. For small, medium, and large organizations it is common to find security teams lacking the fundamental and necessary resources to secure their environment and implement advanced security solutions to combat the modern threats they face. In 2015, we forecast that many businesses will explore strategic security partnerships with trusted and reliable Managed Security Service Providers (MSSP).

3. Security Moves to Big Data and Bleeding Edge Technology

In 2014, we saw Big Data SIEMs leveraging Hadoop, Elastic search, and next generation security tools and platforms like CounterTack Sentinel and Splunk make massive strides in the cybersecurity market space. Additionally the increase in network complexity has rendered most traditional security mechanisms ineffective in carrying out their intended functionality. In 2015, we forecast that Big Data will become a fundamental requirement for security and significant ground will be made on the research and development of bleeding edge cybersecurity artificial immune system technology.

2. Enterprises Develop Response Plans for Ransomware

Last year we saw an increase in ransomware incidents through self-replicating malware designed to encrypt corporate data and give attackers a platform to demand bitcoin payments to release the data. These attacks are very lucrative with higher infection rates driving higher income for the attackers. In 2015, we forecast that ransomware will evolve to target endpoints that subscribe to cloud-based storage solutions and attempt to exploit user sessions to encrypt data stored in the cloud. With no effective security measures against these attacks in sight, we will see companies place a greater emphasis on business continuity and disaster recovery planning programs to anticipate and counter the risk of ransomware attacks.

1. Boards Demand Greater Accountability from Security Teams

After a series of high-profile data breaches in 2014, corporate boards across the world are waking to cyber threats and are grappling with security issues they once relegated to technology experts. Given the increasing frequency of cybersecurity incidents, and the growing impact of those incidents on business, boards are having to increase their security oversight. In 2015, we forecast that board of directors will be more involved and provide direct oversight on steps to quantify, validate, and effectively manage cybersecurity risks in their business.

Created by CyberSheath

Co-founded by a Chief Information Security Officer for a Global Fortune 500 company & Chief Executive Officer for an Inc. 500 company, CyberSheath applies business discipline to cyber security, enabling our customers to measure risk, meet compliance goals, prioritize investments, and improve overall security posture.

We've built a global network of best-in-class partners that we leverage as a force multiplier to deliver pragmatic, end to end solutions for our customers. Having been in the trenches as security practitioners and business executives, CyberSheath goes beyond the WHAT (best practices) and delivers the HOW (measurable results).

Contact

CyberSheath Services International, LLC
11710 Plaza America Drive, Suite 2000
Reston, VA 20190
www.cybersheath.com
1-855-384-8070