This year’s headlines made it clear: the number of devastating cyber-attacks is increasing and the costs aren’t just financial. Every data breach can irreversibly damage an organization’s reputation, a priceless commodity. In this high risk threat landscape, protecting your data from malicious attacks requires not only the right tools, but a pre-emptive awareness of the latest threats and tactics. Below are Websense’s 2015 Security Predictions - eight critical cybercrime trends that will challenge IT security professionals everywhere.

1. **Healthcare Hacks Will Escalate.** Highly valuable Personal Identifiable Information (PII) in healthcare databases will make the industry a prime data theft target. 
   - insurance company, pharmaceutical, hospital and doctor office networks will provide multiple potential entry points for hackers.

2. **Internet of Things (IoT) Attacks Will Focus on Businesses, Not Consumers.** More than sixteen billion devices will be connected to the Internet by 2015 and will double to more than forty billion devices by 2020. 
   - As the attack surface increases, so does the “noise” that must be accurately filtered to identify true threats.

3. **Credit Card Thieves Will Evolve into “Information Dealers” for the Black Market.** Cybercriminals will serve as ‘one-stop shops’ for identity theft and financial fraud with credential-stealing operations harvesting information from a variety of sources. 
   - A ‘result, two-factor authentication will become more commonly required to prevent unauthorized access to data.

4. **Mobile Threats Will Target Credentials.** Mobile devices will be targeted for credentials to Cloud-based enterprise applications and data resources accessed by mobile phones often through auto-login capabilities on mobile apps.

5. **Old Source Code Opens Doors to New Exploits.** Internet threat models show that the underlying source code and protocols are vulnerable to exploitation and will be, leveraged by hackers. 
   - Every update and integration of the old source code will continue to create or expose areas of weakness for hackers to manipulate.

6. **Email Threats Will Be More Evasive and Sophisticated.** Email-borne attacks designed to evade modern email security solutions that look for spam, viruses, and malware will be the new norm. 
   - Email will be an integral part of the threat reconnaissance stage to validate credentials and lead to more effective threat prevention.

7. **Common Collaborative Tools Will Become Cover for Command and Control Infrastructure.** Social networks will provide a target-rich environment for individuals to be impersonated, allowing hackers to gather more data, faster. 
   - Widespread adoption of interactive collaborative tools such as Google Docs will make attractive threat vectors for extending Command and Control Infrastructure.

8. **New Cybercrime Players Will Vie for Superiority and Subterfuge on the Cyber Battlefield.** Increased global connectivity will open opportunities for cybercriminals worldwide. 
   - Cybercriminals will strive into ‘data mercenaries,’ stealing national and corporate secrets to be made available to the highest bidders.

---

Download the full report from www.websense.com/2015Predictions