Social Media Monitoring in Healthcare

The use of social media is on the rise throughout our society, and with good reason. Twitter, Facebook and other popular social media platforms offer a highly-effective way to provide customers and interested parties with information updates, answers to frequently asked questions and breaking news. Other benefits include real-time interaction, broader distribution and sharing of information. But along with its numerous advantages, social media also comes with a down side.

Hackers from across the street or across the globe may attempt to impersonate your organization, post false information or malicious files, attempt to gain insider access, conduct scams to steal money or information from unsuspecting individuals or launch other damaging attacks. Organizations need to find ways to balance a healthy social media presence while safeguarding against constant threats.

ACHIEVING FULL 360-DEGREE PROTECTION

CGI's end-to-end fraud, waste and abuse solution applies a holistic approach to some of the most vexing issues facing the healthcare industry today. Our proven methodologies and proprietary technologies help fuel not only prepay and post-pay solutions but also reimbursement services that educate payers on how to improve error rates and create better policy and billing practices moving forward.

The key to CGI's holistic approach, however, is how we incorporate Social Media Protection Services—using analytics and secure cloud solutions—for an extra layer of protection. This allows CGI to identify, detect and scrub improper activities on social media sites across a wide array of venues in real time to keep your organization safe.

If an inappropriate action has been detected, steps are immediately taken to minimize the impact of a breach or misuse of social media accounts. This protection allows our customers to enjoy full 360-degree, 24/7/365 protection, which not only translates into dollars and cents but also total peace of mind.

THE SOCIAL MEDIA MINEFIELD

Organizations today understand that social media plays a huge role in how they can interact with and inform their constituents.

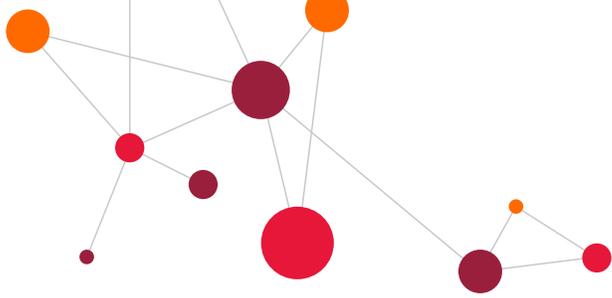But some still may not be convinced about how widespread the problems are.

The numbers, however, back it up:

#1 Targeted social media malware is the number one method for **breaching** a network

40% Of enterprises have fallen victim to social media **spearphising** attacks

20% Or 1 in 5 organizations have been infected with **malware** sent via social media

cgi.com

PROVIDING AUTOMATED THREAT DETECTION AND MONITORING

Through predefined policies, CGI is able to provide automated threat detection and monitoring to help with:

- **Information Security:** Targeted phishing and malware attacks, social engineering, asset security and visibility, account hijacking and executive impersonations.

- **Threat Intel and Chatter:** Executive protection, physical security, threat actor intelligence, social DLP, hacktivism, travel security.

- **Fraud and Customer Protection:** Stock manipulation, financial scams, card cracking, fake coupons, fake support reps, identity theft.

- **Brand Protection:** Offensive content, trademark infringement, corporate impersonations, spam.

- **Loss Prevention:** Piracy, counterfeit goods, illegal streaming, bot removal.

DELIVERING REAL-WORLD RESULTS FOR OUR CLIENTS

CGI recently conducted a 5-day pilot program for one of its customers that had experienced an incident. During the pilot period, CGI's social media monitoring platform consumed and analyzed 2,200 posts, 11,200 accounts, 4,200 links and 1,800 images.

The system generated more than 500 alerts related to impersonating accounts, suspected fraud and suspicious domains. The organization was targeted by foreign threat actors (e.g., Russia, China) and it was determined that executives were susceptible to impersonation on social media.

During this period, CGI was able to successfully demonstrate the ability to:

- Identify impersonations of client on social and digital channels.
- Identify suspected fraud against client on social and digital channels.
- Identify impersonations of selected client executives on social and digital channels.
- Monitor the Deep/Dark Web for mentions of client that are associated with pre-defined fraudulent terms.

The results of the pilot goes to show that while social media poses a real and significant threat to an organization's brand and reputation, CGI will protect customers every step of the way by providing proven, effective solutions to combat this growing cyber problem.

PROTECTING ALL OF YOUR VALUABLE SOCIAL MEDIA ASSETS

CGI's proven social media monitoring can help reduce operational costs and reduce the time it takes to time to identify a threat, investigate, and clean up an issue as well as increase the breadth of your defense-in-depth program.

OUR MANAGEMENT CONSULTING SERVICES

- Financial Management
- Operations Strategy
- Business Transformation
- Shared Services
- Change Management
- Program Management
- Advanced Analytics
- Performance Management
- IT Advisory Services

To learn more about our services or to schedule a discussion, please contact info@cgifederal.com.

cgi.com
© 2019 CGI INC.