ISSUE 5

Securely Speaking:

Your Privacy & Security Bulletin

BY **REBOOT COMMUNICATIONS LTD.**
WITH FOUNDING SPONSOR **GOSECURE**

1. **A Case for AI Security as a Practical Counterpart to Responsible AI**
2. **Elevating Cybersecurity with the MITRE ATT&CK Framework:** *A Strategic Approach to Threat Modeling*
3. **The Human Factor in Cybersecurity:** *Addressing Vulnerabilities through Innovative Training*

Reboot COMMUNICATIONS LTD

info@rebootcommunications.com

GoSecure

WWW.REBOOTCOMMUNICATIONS.COM

Forward

Welcome to ***Securely Speaking: Your Privacy & Security Bulletin***, a regular quarterly publication provided by Reboot Communications Ltd. The bulletin's objective is to explore the latest trends and developments in privacy and security, including the challenges and opportunities that arise from new technologies like artificial intelligence, the Internet of Things, and blockchain. We also examine the legal and ethical implications of data collection and use, and look at how organizations and individuals can take steps to protect themselves and their information.

We invite you to review articles and interviews which will provide our readers with a comprehensive understanding of the complex and evolving landscape of privacy and security, as well as actionable advice and best practices for navigating it.

We believe that a better understanding of these issues is crucial for all individuals, organizations, and governments, and that by fostering a dialogue around privacy and security, we can work together to create a safe, more secure, and more ethical future for all. We hope you enjoy reading this bulletin and join us in this important conversation.

We focus on these strategic pillars to provide a comprehensive and valuable resource for staying informed and protected in the digital age:

OUR KEY STRATEGIC PILLARS

Education & Awareness/ Best Practices

Educating readers on the latest privacy and security threats, best practices, and emerging trends.

Thought Leadership & Industry News

Articles and interviews with experts in the privacy and security field.

Emerging Technologies

Emerging technologies and their potential impact on privacy & security (ie AI, IoT, blockchain).

Regulatory Developments

Information on the latest privacy and security regulations and laws.

Case Studies

Real world examples of privacy and security breaches and how they were addressed.

Acknowledgements

ARTICLE 01

A Case for AI Security as a Practical Counterpart to Responsible AI

By: **Sara Faradji** | Cybersecurity Technical Content Manager, Optiv
Brian Golumbeck | Practice Director, Strategy and Risk Management, Optiv
Randy Lariar | Practice Director, Big Data, AI and Analytics, Optiv

ARTICLE 02

Elevating Cybersecurity with the MITRE ATT&CK Framework:
A Strategic Approach to Threat Modeling

By: **Troy Vennon** | Director of Service Innovation, GoSecure

ARTICLE 03

The Human Factor in Cybersecurity:
Addressing Vulnerabilities through Innovative Training

By: **Gregory Carpenter** | Chief Security Officer, KnowledgeBridge International

ARTICLE 1

A Case for AI Security as a Practical Counterpart to Responsible AI

Image by freepik

Artificial intelligence (AI) products and capabilities are growing at an unprecedented pace, transforming the way we work and interact with technology. Large-scale frontier AI models are at the forefront of innovation in this evolving space, with products from Google, OpenAI, Microsoft and Anthropic facilitating more advanced human-computer interaction than ever. Not only can people use open-source generative AI (GenAI) tools to simplify workflows, proofread text and design images, but they can also code games, build prototypes and more. We also find ourselves using AI capabilities regularly in our smartphones, word processors and video meeting spaces as vendors deploy new AI features into their products.

As AI demand persists, it is important to take a step back and reflect on the ethics surrounding AI use. Technology providers, lawmakers, academics and other stakeholders are actively exploring strategies to **ensure that AI helps more than it harms society**. Data integrity, privacy and security around AI models and applications are central to the global discourse on "responsible AI." This methodology focuses on strategic decision-making to reduce AI risk and the likelihood of causing harm, while upholding **principles of fairness, accountability and trust**. But there are many competing definitions of trustworthy, responsible and fair AI. Under pressure to innovate quickly while earning user trust, organizations and individuals alike must make practical decisions today as the ethical landscape surrounding AI rapidly changes. AI security overlaps with conversations on responsible AI, but it is imperative to recognize key distinctions between the terms when maximizing an AI investment. To elucidate the significance, we examine the limitations of responsible AI before exploring the practical applications of AI security in everyday use cases.


Image by freepik

Responsible AI ≠ Secure AI

While both responsible AI and AI security are essential to critical decision-making on the safe, trustworthy use and deployment of AI, it is critically important to understand how the concepts differ and which one your organization needs to focus on to ensure AI success.

Responsible AI prioritizes a strategic emphasis on ethical and societal impacts of AI. Privacy and compliance leaders at top technology companies are actively working to define what responsible AI looks like when building their frontier AI models. They are devising ways to reduce bias, misinformation, regulatory violations and legal liabilities

for both current and future AI users. Evolving discourse on responsible AI is vital for ensuring that companies demonstrate transparency and accountability as they earn and maintain user trust in their products.

Responsible or ethical AI cannot be achieved without AI security. Security in this context not only prioritizes availability and confidentiality, but most importantly here, integrity.[1] Focusing more on proactively identifying and mitigating AI-related cybersecurity risk, the goal of AI security is to protect AI systems and data from malicious use by both internal and external cyber threat actors. To address these risks, AI security can be incorporated within security operations, data security, infrastructure security, application security and other critical areas.

The objectives of responsible AI and AI security both center on maximizing the benefits of AI while reducing risk. Where they differ, however, is in their methodological approach. Responsible AI is more of a theoretical set of ideas aligned on ethical decision-making surrounding AI use and development. AI security, on the other hand, brings the discourse on responsible AI to more practical applications of cybersecurity risk mitigation. The terms may seem black and white in their distinctive approaches. **But as the image on the next page illustrates, they are part of a spectrum of AI risk management.**

Bridging the Gap with AI Security

While responsible AI and AI security share similar goals in implementing AI governance principles for an organization, not every business has the resources to invest in both. Large-scale frontier AI model developers are prioritizing responsible AI to lower the risk that their extensive user base may receive and share inaccurate or biased results from their products. But for many enterprises and small businesses, responsible AI may not be the most practical investment.

To tangibly support the people in your organization, you need more than just the guiding principles and ethical considerations of responsible AI; you need experienced professionals who can protect your business from AI-related risk. For developers, this means embedding safety measures throughout the AI build process to ensure end-to-end security by design. For users, this means having clear, hands-on guidance and training from your organization on company-approved AI use cases and policies. Although AI security may be more focused on cybersecurity than ethical decision-making, it nonetheless has a broader application throughout the business.

REFERENCE:

[1] ***MITRE ATLAS™*** *defines AI security as "the tools, strategies, and processes implemented that identify and prevent threats and attacks that could compromise the confidentiality, integrity, or availability of an AI model or AI-enabled system." Building upon their emphasis on the "CIA triad" (confidentiality, availability and integrity) that is a central information security framework, Optiv especially finds value in the focus on integrity in AI security.*

Responsible AI

Regulatory
AI causes a breach of regulatory obligations, incurring fines and potential business disruption

Overreliance on AI
Misinformation, miscommunication, legal issues and security vulnerabilities result from excessive dependance on LLM

Excessive Loss of Money
AI is manipulated to incur excessive costs

Legal/IP Risk
AI exposes the firm to legal liabilities due to failure to follow existing legal or through the incorporation of models built with non-licensed third-party IP

Inaccurate Results (Hallucination)
AI makes up false information or facts that are not based on real data or event

Bias
AI provides outputs that discriminate against race, gender, socioeconomic status or other demographic factors and prevents unbiased outcomes to customers and stakeholders

Malicious Models
Using models containing malicious code, backdoors or hidden behaviors

Model Extraction/Inversion
Exposes information about the training data or algorithm

Input Spoofing
Fools vision/image classification, facial recognition, fraud and spam detection

Secure AI

Backdoors
Contaminate or poison training data to implant hidden triggers

Reprogramming/Detraining
Alters system behavior through real-time input tampering

Weak Algorithms
Selecting an algorithm with known vulnerabilities

Training Data Poisoning
Bad actors gain access to training datasets and tamper with the intended outcome by injecting false data

Shadow AI
AI that is created outside of governed processes and that can expose the firm to additional risks including security, regulatory, operational and reputational

Prompt Injection
A third-party hijacks the LLM output to alter its response

Insecure Supply Chain
Attackers influence the data, model or technology inputs to AI to achieve data exfiltration or disruption

Denial of Service
A cyberattack makes a machine or network resource unavailable to its intended users

Data Leakage – Privacy
Personally Identifiable Information (PII) and health information may be exfiltrated via AI to third-party tools or attackers

Data Leakage – IP
Sensitive and/or proprietary data may be exfiltrated via AI to third-party tools or attackers

Practical Use Cases for AI Security

To better understand the real-world value of AI security, consider what you need to measure the success of your AI solution. Whether you are seeking to maximize productivity and safety for AI users or developers, the following examples illustrate ways that AI security can help you practically achieve business outcomes.

User Outcomes

Users include: leadership, functional business leaders, employees

The correlation between widespread use of third-party GenAI tools and cybersecurity attack surface augmentation is not always obvious, but AI security helps organizations protect users from harm with AI governance, literacy and training.

Upskill your team

Leverage the benefits of AI and clearly outline specific use cases to support user productivity and upskilling. Boost workforce confidence and efficiency in ethical enterprise AI use with training and education.

Foster employee trust

The benefits of AI can only be realized if the product users trust the results. Explainable AI, which is built on a foundation of trusted IT systems, is required to ensure employee adoption.

Mature your AI security

Enhance your security for existing risk management practices, including threat models, risk assessments and risk registers to effectively address AI use cases.

Build AI security resilience

Evaluate AI models, applications and APIs to uncover and mitigate vulnerabilities for more secure AI use throughout your organization.

Integrate AI security in the SDLC

Strengthen the security of practices across the SDLC, as well as the integrity of content for users who are writing code or building applications using GenAI.

Model Developer Outcomes

Recognizing your priority in building cutting-edge AI models and innovating quickly to keep up with market demand, AI security helps ensure your models are reliable and safe while reducing your company's risk for security and compliance issues.

Build AI security from the start

Become an AI-enabled organization and have comprehensive answers and plans to address governance, privacy and risk exposure when fielding inquires and situations requiring immediate action.

Secure business value in the modern data era

Ensure appropriate guardrails with solid data governance through safe, scalable AI use rooted in transparency and respect for data privacy.

Accelerate innovation without compromising risk

Confidently develop and integrate AI capabilities that limit your risk exposure—saving you the time and money that would be involved in reactively mitigating existing risk.

Secure AI to Achieve Business Outcomes

As public discourse surrounding responsible AI evolves, what is most valuable for you to consider is what you want most out of your AI investment. It is important to prioritize AI risks before they become the source of security incidents or compliance concerns. Responsible AI advisory services are key for setting internal policies and standards aligned to your core values. AI security services provide both the advisory and practical components for AI strategy, governance, training, vulnerability management, threat modeling, risk management and more.

By: Sara Faradji | Cybersecurity Technical Content Manager, Optiv
Brian Golumbeck | Practice Director, Strategy and Risk Management, Optiv
Randy Lariar | Practice Director, Big Data, AI and Analytics, Optiv

At **Optiv**, we want to hear your questions and ideas about comparisons between responsible AI and AI security. Email us at AI@optiv.com to continue the conversation with AI security experts.

For additional information on services, visit **www.optiv.com/AI**.

VISS VANCOUVER INTERNATIONAL SECURITY SUMMIT

Vancouver, BC

Corporate Sector, Law Firms, Diplomats, Policy Groups, Academia, Public Sector

Nov. 25-26, 2024

Foreign Threats – Economic & Political Resiliency

Global subject matter experts to discuss the following:

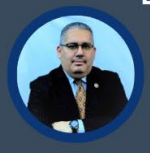
- ForeignThreats Geopolitical Conflict
- Critical Infrastructure Resiliency
- CyberSecurity State-Sponsored Threats
- Financial Crimes & Money Laundering
- Economic Coercion and Subversion
- Lawfare Vulnerabilities & Legal Resiliency
- Misinformation / Disinformation
- Economic, Political & Legal Partnerships

Keynote Speakers

Tricia Geddes
Deputy Minister (Incoming)
Public Safety Canada

Sami Khoury
Government of Canada
Senior Official for Cyber Security

Dr. Vlasta Zekulic
Branch Head, Strategic Issues and Engagements, NATO Allied Command Transformation



David Luna
Founder and Executive Director, ICAIE

David Asher
Senior Fellow
Hudson Institute

Register Now!
www.rebootcommunications.com/event/viss2024/

Reboot COMMUNICATIONS LTD

ARTICLE 2

Elevating Cybersecurity with the MITRE ATT&CK Framework: A Strategic Approach to Threat Modeling

Image by freepik

As the sophistication of cyber threats grows, organizations can no longer rely on reactive security measures. To stay ahead of attackers, it's essential to adopt a proactive approach – and threat modeling with the MITRE ATT&CK framework provides a structured, data-driven way to do so. This method enables security teams to align their defenses with real-world adversary tactics, offering more precise and actionable insights into how to improve security posture.

But how exactly does the MITRE ATT&CK framework work, and why is it so effective in enhancing cybersecurity strategies?

Understanding the MITRE ATT&CK Framework

The MITRE ATT&CK framework is a comprehensive tool that categorizes adversarial tactics and techniques based on real-world observations. While many cybersecurity professionals are already familiar with threat modeling, ATT&CK takes this a step further by offering a unified view of how attackers behave at various stages of an attack. Instead of focusing on isolated security controls, this framework provides a more granular understanding of how threat actors achieve their goals with defined Tactics and Techniques.

For instance, while the Lockheed Martin Cyber Kill Chain offers a linear view of an attack, MITRE ATT&CK breaks down specific adversarial techniques used at different stages. This detailed view allows organizations to better understand how threats operate, enabling more effective and targeted defenses.

The Role of Threat Modeling in Cybersecurity

One of the primary benefits of threat modeling with MITRE ATT&CK is that it helps bridge the gap between governance, risk, and compliance (GRC) programs and the technical controls (tools or configurations) we employ as defenses. Too often, security solutions are implemented based on vendor recommendations rather than an understanding of the actual threats organizations face. Penetration tests might offer some insights, but they can't fully evaluate every tool or endpoint in your environment.

By mapping specific adversarial techniques to your security controls, organizations can move beyond vague assurances like "We pen-tested the network this year" and instead provide concrete data. For example, a security leader could state, "Our defenses are 88% effective against this particular technique," offering a clearer, more accurate picture of security efficacy.

Moving from Reactive to Proactive Security

Traditionally, threat modeling has been used to ensure software applications are built with well-written, secure code and strong security controls. However, identifying which threats these controls should defend against has often been a challenge. The MITRE ATT&CK framework helps solve this issue by providing a way to map adversarial tactics and techniques to specific security controls, making it easier to evaluate whether defenses are effective.

Consider this: If ransomware is a top concern for your organization, you can use the MITRE ATT&CK framework to identify common techniques used by ransomware groups and assess how well your defenses hold up against these methods. By understanding which techniques are most likely to be used by attackers targeting

your industry – whether it's healthcare, finance, or manufacturing – you can allocate resources more effectively to plug any gaps in your defenses.

The Power of Collaboration and Intelligence Sharing

Another advantage of the MITRE ATT&CK framework is its ability to foster collaboration across industries. Many organizations have traditionally relied on Indicators of Compromise (IoCs) for threat intelligence sharing, but ATT&CK enables a more structured approach. Companies can now communicate more clearly about the tactics adversaries use and share insights on how to counter these threats.

Initiatives like industry-specific Information Sharing and Analysis Centers (ISAC) or Information Sharing and Analysis Organizations (ISAO) in the United States exemplify how ATT&CK enables companies to collaborate more effectively, developing stronger defenses against shared threats. By using a standardized framework, organizations can share data on the adversarial techniques they've encountered, leading to better collective security outcomes.

Image by freepik

Continuous Improvement and Quantifying Risk

One of the core strengths of the MITRE ATT&CK framework is that it facilitates continuous improvement. Security isn't a one-time project – it requires ongoing assessment and refinement. By regularly mapping your controls to adversarial techniques, you can continually evaluate the effectiveness of your defenses and identify areas for improvement.

For example, after mapping your controls to specific MITRE ATT&CK techniques, you might discover a gap in your defenses against a high-risk threat. Armed with this knowledge, you can secure the necessary resources, implement new mitigations, and test them to ensure they're effective. This ongoing process ensures that your defenses remain current and aligned with the latest adversarial techniques.

Example of identified gaps in coverage for adversarial techniques:

From Strategy to Execution: The Strategic Kill Chain

Aligning strategic cybersecurity goals with tactical execution is another key benefit of using MITRE ATT&CK. By mapping out techniques like credential dumping or lateral movement, organizations can prioritize their investments in controls that will have the greatest impact on security. This alignment ensures that your defenses are focused on the areas where your organization is most vulnerable, improving overall security efficacy.

The Path Forward: Adopting a Threat-Informed Approach

As cyber threats continue to evolve, adopting a threat-informed strategy with the MITRE ATT&CK framework becomes essential for staying ahead of adversaries. By aligning defenses with real-world adversarial techniques, organizations can ensure their security programs are both effective and proactive.

By regularly updating threat models, conducting offensive testing, and validating security controls, organizations can quantify their security posture and make informed

decisions about where to allocate resources. This structured, data-driven approach provides both executives and security teams with the actionable insights they need to stay ahead of emerging threats and make informed decisions about where to allocate resources. This structured, data-driven approach provides both executives and security teams with the actionable insights they need to stay ahead of emerging threats.

Conclusion

Threat modeling with the MITRE ATT&CK framework offers a smarter, more proactive approach to cybersecurity. It empowers organizations to move beyond reactive measures, providing clear insights into the tactics used by adversaries and aligning defenses accordingly. As cyber threats become increasingly sophisticated, adopting a threat-informed, continuously improving strategy will be crucial for maintaining a strong security posture.

By incorporating the MITRE ATT&CK framework into your threat modeling process, your organization can better anticipate threats, optimize security controls, and ultimately stay ahead of attackers.

By: Troy Vennon | Director of Service Innovation, GoSecure

ARTICLE 3

The Human Factor in Cybersecurity: Addressing Vulnerabilities through Innovative Training

Image by rawpixel.com on freepik

Introduction

Digital transformation is rapidly reshaping the cybersecurity landscape, driven by advancements in artificial intelligence and the impending implementation of quantum capabilities. As organizations navigate increasingly sophisticated cyber threats, it becomes essential to recognize that human error remains one of the most significant vulnerabilities within cybersecurity frameworks. The complex interaction of numerous factors contributing to human error in security breaches highlights the need for innovative training solutions to mitigate these vulnerabilities.

While substantial investments in advanced technologies – such as firewalls, intrusion detection systems, and encryption – are crucial, they are insufficient. Human behavior is a critical element often overlooked but significant in many security incidents. Understanding the primary causes of human error highlights the importance of effective training and assessment methods, emphasizing the need to focus on the human element.

Understanding Human Error in Cybersecurity

Research indicates that human error is a leading cause of security breaches. The 2022 Verizon Data Breach Investigations Report found that human error was implicated in approximately 82% of data breaches, highlighting the need for organizations to address vulnerabilities coming from within their workforce.

Human error manifests in several ways:

- **Negligence:** Employees may fail to follow established security protocols, such as using weak passwords or neglecting software updates.
- **Lack of Awareness:** Many employees do not recognize potential threats like phishing scams or social engineering tactics.
- **Misunderstanding of Protocols:** Inadequate or infrequent training can result in misinterpretation of security policies, causing improper handling of sensitive information.

Understanding these indicators is crucial for developing effective mitigation strategies.

Image by freepik

Image by DC Studio on freepik

Innovative Training Solutions

To address the vulnerabilities associated with human error, organizations must prioritize innovative training solutions that are engaging, relevant, and adaptive.

Here are a few effective strategies:

1. **Interactive Training Modules:** Traditional training methods often rely on passive learning techniques, leading to disengagement. Incorporating interactive elements like gamification and simulations can enhance employee engagement and retention. For example, security awareness games can simulate real-world scenarios, allowing employees to practice identifying threats in a safe environment.
2. **Micro-Learning Approaches:** Delivering content in small, digestible units helps employees learn information without feeling overwhelmed. This approach is effective in cybersecurity training, where the landscape constantly evolves. Short, focused sessions on specific topics – such as recognizing phishing emails or proper data handling – can improve comprehension and retention of critical skills.
3. **Continuous Learning and Regular Updates:** Given the dynamic nature of cyber threats, training programs must be adaptable. Organizations should implement continuous learning opportunities, such as monthly refreshers or on-demand resources, to keep employees updated about the latest threats and best practices. This proactive approach reduces the likelihood of human error.
4. **Role-Based Training Customization:** Tailoring training programs to specific organizational roles ensures that employees receive relevant information applicable to their responsibilities. For instance, IT staff may require in-depth technical training, while customer service representatives may need a focus on social engineering and customer data protection.

5. **Cultivating a Cybersecurity Culture:** Creating a strong organizational culture that prioritizes cybersecurity fosters a proactive mindset among employees. Leadership commitment to cybersecurity initiatives, open communication regarding security concerns, and recognition of good practices reinforce the importance of individual responsibility. Employees who view cybersecurity as a shared responsibility are more likely to remain vigilant.
6. **Phishing Simulations and Real-World Testing:** Regular phishing simulations can effectively educate employees about email threats. Organizations can gather valuable data on vulnerabilities and provide targeted feedback by testing employees' ability to identify phishing attempts. This practical experience enhances awareness and readiness to respond to actual threats.

Measuring the Effectiveness of Training

Cybersecurity is an essential priority and requires executive buy-in because it directly and significantly impacts the organization's bottom line. Even today, executives must remember that investing in robust cybersecurity protects sensitive data and enhances the company's overall financial health. By gaining executive buy-in, organizations can implement strategies that lead to measurable improvements in their security posture.

To effectively gauge the success of these strategies, it is crucial to establish metrics that demonstrate the return on investment of cybersecurity initiatives. Measuring the effectiveness of training programs is a vital component of this process.

Key metrics to consider include:

- **Phishing Click Rates:** Monitoring the percentage of employees who click on simulated phishing emails before and after training provides a clear insight into the training's impact.
- **Incident Response Time:** Assessing how quickly employees report potential threats indicates their awareness and understanding of security protocols.
- **Feedback Surveys:** Gathering employee feedback on training programs helps identify areas for improvement and ensures that the content resonates with staff.

Conclusion

As organizations navigate the complexities of the digital age, addressing the human factor in cybersecurity is crucial. Human error remains a significant vulnerability, and innovative training solutions are essential for mitigating risk. By adopting engaging, role-based, and continuously updated training programs, organizations can empower their employees to become proactive defenders against cyber threats. Everyone can defend.

By: Gregory Carpenter | Chief Security Officer, KnowledgeBridge International

Since its founding in 2008, **KnowledgeBridge International (KBI)** has excelled in developing innovative operational technologies and concepts to meet the innovative requirements of its clients. KBI offers a broad range of services, from tactical technology solutions using user-friendly rapid prototyping tools to strategic initiatives in multi-INT anticipatory intelligence and cyber defense while maintaining a strong reputation for consistently high performance.

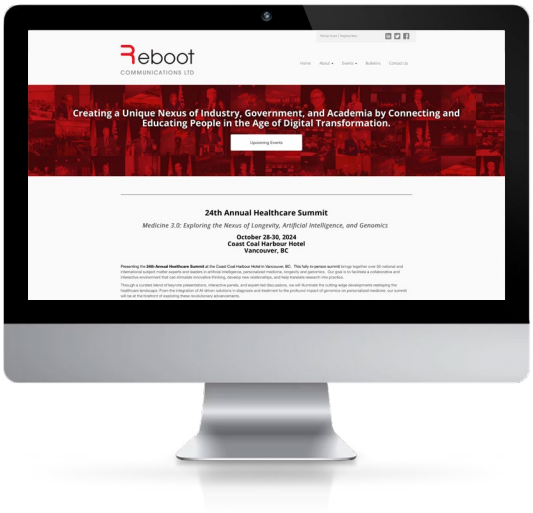
KBI prioritizes collaboration with academic researchers to tackle complex challenges, providing consulting services focused on emerging cyber capabilities and their implications. KBI's offerings include custom mobile app development, tailored hardware solutions for law enforcement and military needs, and comprehensive training programs to help users navigate rapid technological changes.

KBI's core competencies are in systems integration, information systems architecture, and vulnerability analysis to address the evolving threats posed by technology. The company emphasizes engineering support services that empower clients to understand their needs, facilitating informed decision-making and fostering resilience against cyber threats.

Copyright

ISSUE 5 EBOOK EDITION | *OCTOBER, 2024*

Editor: **Greg Spievak**



FIND OUT MORE & SUBSCRIBE

For more information or to subscribe and receive the ***Securely Speaking: Your Privacy & Security Bulletin*** regularly, email info@rebootcommunications.com.