

IANS 2012

Dave Shackelford

Senior Vice President & Chief Technology Officer, IANS

As the information security community looks at the year ahead, what is top of mind? What is most pressing for security teams? Based on in-depth discussions with our clients, Faculty, and numerous security experts in the field, IANS has uncovered the most relevant topics for 2012. We have put together a hard-hitting research agenda that will bring you real, tactical insights, and information you can put to use for budgeting cycles, improvements in your operations, and longer-term strategic planning with both business units and IT leadership.

Cloud Security is one of the most pressing concerns for many organizations, as business units look to move applications, systems, and data into cloud provider environments. What kinds of technical, legal, and operational challenges do security teams need to think about, and how can we overcome them? IANS will be focusing on this from every angle, working closely with industry experts and groups like the Cloud Security Alliance (CSA).

Questions we'll be addressing on Cloud Security:

- What kinds of cloud controls frameworks are best suited to enterprise environments, and how do they align with compliance mandates?
- What kinds of cloud governance models work best in large organizations?
- What kinds of tools and techniques are available for encrypting data in the cloud?
- How can we improve data breach and incident response tactics for our cloud-based assets?
- What kinds of cloud-based security offerings will be available, and how mature are these?

Mobile Device Security is proving to be a huge and growing area that shows no signs of slowing down. Over 2011, many security executives we spoke with indicated that mobile device management, new mobile device malware, and the definitive interest their organizations show in "Bring Your Own Device" (BYOD) use cases are leading them to new risk scenarios that are challenging, to say the least. IANS will strive to provide in-depth technical insights about new cutting-edge tools and methods to improve your mobile device security program.

Questions we'll be addressing on Mobile Device Security:

- What mobile device technologies are available today, and what kinds of capabilities do they have? What new technologies are emerging?
- How can we identify rogue or malicious mobile apps from the Android or Apple App Stores? How can we prevent and detect installation of these apps?
- What kinds of mobile malware is being seen in the wild? What new capabilities are attackers developing?
- What kinds of legal and compliance considerations are organizations facing as they look to implement BYOD?
- What kinds of cloud-based security offerings will be available, and how mature are these?

Security Metrics have proven difficult to identify for many organizations. Beyond choosing the best metrics that work, measuring and reporting specific data can be a real problem for many. What types of information are most useful to business units and executive leadership? What trends and data will help security operations improve over time? There are numerous efforts underway in the industry to improve the state of security metrics, but are any of them working? IANS will be working hard to bring you the most current and relevant metrics programs that work, along with ideas you can use for improving your current metrics.

Questions we'll be addressing on Security Metrics:

- How do we get started with building a meaningful metrics program? What are best practices for security metrics programs?
- What metrics are most useful to business management, and how do we most effectively convey risk using these?
- How can we analyze large quantities of security data and distill sound metrics in an automated fashion?
- What analysis techniques work best, and how can we create and improve metrics-based security scorecards?

SCADA and Critical Infrastructure Attacks are increasing. With the advent of Stuxnet, and later Duqu, security teams are realizing that well-funded attackers are creating very specific malware aimed at critical infrastructure. The impact to all organizations is enormous, with the potential for catastrophic failures in utilities, transportation, and even medical sectors, to name a few. IANS' research agenda will include updates on what's happening in this important area, keeping you informed and knowledgeable about the latest trends, and how they impact you.

Questions we'll be addressing on SCADA and Critical Infrastructure Attacks:

- How do critical infrastructure security issues affect enterprises? What are the unique risk profiles and concerns enterprise security teams should be focusing on?
- What types of attacks are emerging that threaten critical infrastructure? What are critical infrastructure vendors doing to improve security in their products?

Data Breaches and Incident Response

are areas where most organizations realize they need to improve. How do organizations navigate the sea of new data breach notification laws? What are the trends in legal and compliance ramifications from data breaches? On the technical side, many organizations are looking to improve their response capabilities, seeking to detect incidents more quickly, and respond rapidly as well. With the proliferation of data breaches showing no signs of letting up, and a general dearth of actionable information that security teams can use to improve their response programs, this is a topic IANS plans to tackle with some of the leading minds in the industry in 2012. We'll bring you real-world data about breaches in different verticals, strategies that have worked for some, common pitfalls, and additional insights that can help you plan both short-term and longer-term data breach and incident handling strategies.

Questions we'll be addressing on Breaches and Incident Response:

- What new techniques and tools are available for identifying compromised systems, focusing on HTTP/HTTPS traffic, local system changes, and best practices for analyzing encrypted traffic?
- How do we go about building a Security Operations Center (SOC)? What are best practices for planning, building, and operating?
- What kinds of correlation rules are organizations using to detect anomalies and potential breach behavior in their environments?
- What are best practices for purchasing, implementing, and monitoring SIEM and Log Management tools?

Advanced Threats and Targeted Attacks

have dominated the headlines over the past 2 years. More organizations are experiencing highly sophisticated data breaches with advanced malware, and are coming under fire as targets from coordinated criminal hacking groups. What are the best technologies and processes organizations need to improve their detection capabilities and limit the damage from these attacks? Are there any proven ways to prevent them? What about the increase in social engineering and client software exploitation? Many IANS clients have indicated that improving detection and prevention techniques for these advanced, targeted attacks is a high priority. In 2012, IANS will be working with leading forensics and malware experts to help develop the most practical research possible, with specific focus on things you can put into practice right away.

Questions we'll be addressing on Advanced Threats and Targeted Attacks:

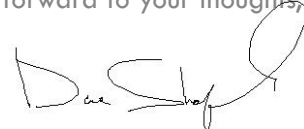
- How are organizations dealing with new, advanced threats?
- Do security awareness programs work at all? If so, what techniques are proving most helpful in combating social engineering attacks?
- What kinds of host-based security tools can help us prevent and identify changes to systems caused by attacks? Can Network Access Control (NAC) tools help prevent further damage?
- What new and sophisticated Web application attacks are appearing, and how can we prevent and detect them?
- How can we improve our Threat Intelligence function? How can we gather better, more actionable data that identifies us as a target?

In addition to these topics, we'll also certainly be covering any number of areas near and dear to security professionals, including the following:

- Curbing data loss across the organization (implementing DLP in the new world of BYOD)
- Making sense of the security data tidal wave (Logging, SIEM, and more)
- Application Security from A to Z, covering development cycles, penetration testing, and everything in between
- Adopting ITIL and other frameworks to security operations
- Taking IT Risk Management from "Marketing Babble" to Implementation
- New developments in IT security architecture, including access controls, network security, host-level security, and more
- Legal and compliance developments that impact you the most, and how to deal with more regulations than ever
- Security operations fundamentals like patching and configuration management, and how we can finally start taming these
- Security awareness programs, why they don't work, and what to do about it
- Forensics tools, processes, and how best to work with law enforcement and other outside groups when you need to
- Thinking offensively, with penetration tests and vulnerability management programs, and finding ways to fend off attackers with smarter, faster defense through aggressive tactics
- Assessing the risk of "hacktivism" and other "online nuisances"
- Charting a strategy that accommodates broken Internet trust models - what happens when we can't trust SSL at all anymore?

And more! We're excited to work with the smartest security minds in the business, as well as security and compliance teams from a broad, diverse range of industries with a wealth of knowledge to share. We're looking forward to bringing you actionable security guidance that can be put to use right away - you won't want to miss it.

I look forward to your thoughts,



Dave Shackelford
Senior Vice President & Chief Technology Officer, IANS

