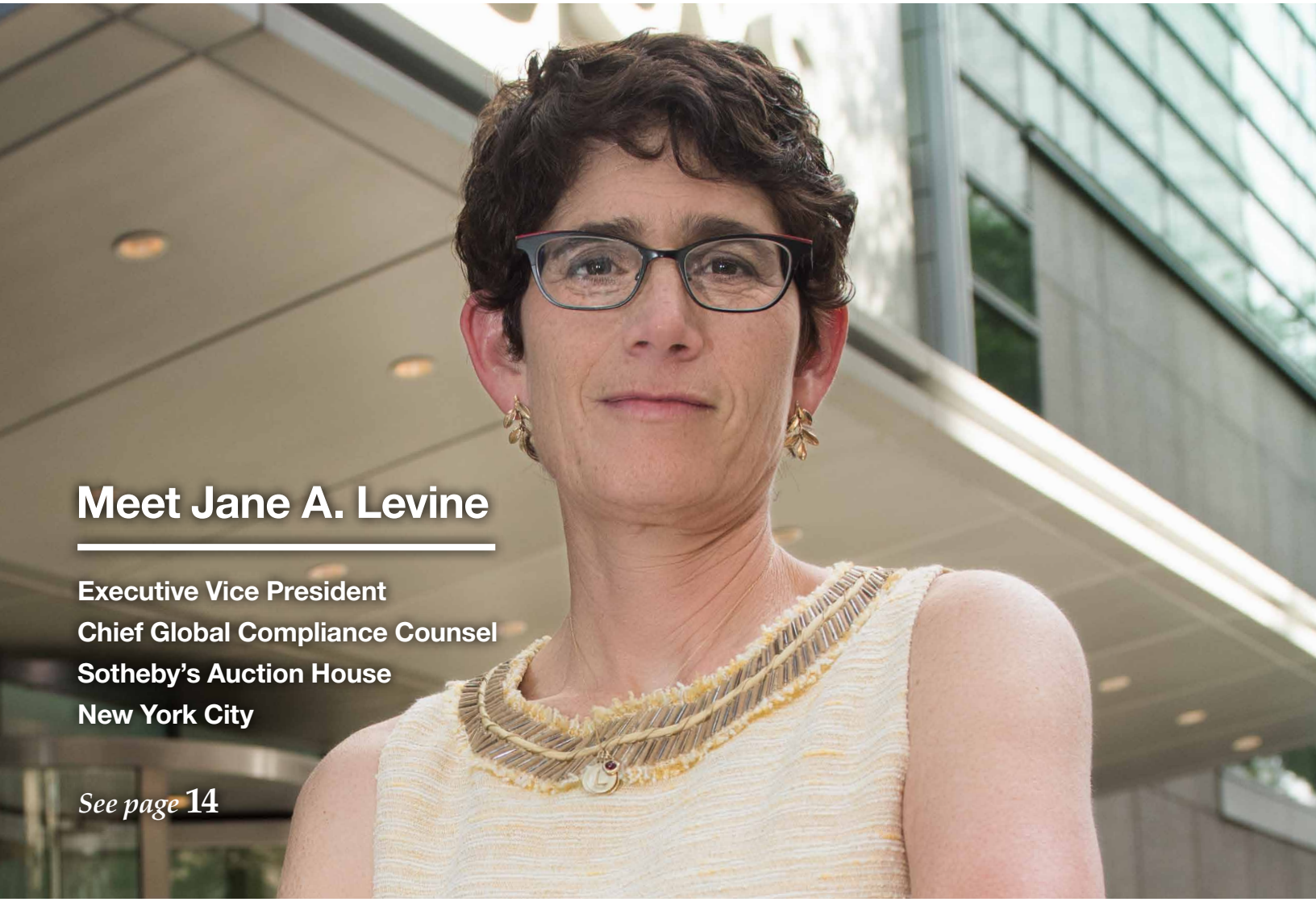
Compliance & Ethics Professional®

September 2016

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

www.corporatecompliance.org



Meet Jane A. Levine

Executive Vice President
Chief Global Compliance Counsel
Sotheby's Auction House
New York City

See page **14**

by Mahmood Sher-Jan, CHPC, CEO, RADAR

Data mishaps: Everyday events, inevitable incidents, and data breach disasters

» It's important to define an event vs. security incident vs. privacy incident vs. data breach.
» Malware and phishing attacks are occurring more frequently.
» Privacy, Compliance, and Security should work together on incident response.
» Proper incident response protects your customers' sensitive data against threats.
» Determining which category these occurrences belong in will help you properly assess the risks of data exposure.

In today's threat-filled world, sensitive customer data is constantly at risk for compromise. Cyber attacks, ransomware, spear phishing, malware, system and process failure, employee negligence, lost or stolen devices—the list of dangers goes on.


Sher-Jan

Indeed, it's a near-certainty that your organization's data will be—or already has been—compromised. But how do you define such an occurrence? Is it an event? A security incident? A privacy incident? A data breach? Does it even matter what it's called?

It absolutely matters. How you label an occurrence that may or may not involve the unauthorized disclosure of sensitive customer data will determine, among other things:

- Should the core or the extended incident response team be involved?
- What containment and remediation actions should be taken?
- Will notification be required or not?
- Who must be notified, when, and how?

These factors will dictate your response, and thus how well you can minimize the monetary, regulatory, and reputational risks to you, your company, and the customers you serve.

Category 1: Events

In its *Computer Security Incident Handling Guide,*[1] the National Institute of Standards and Technology (NIST) defines an event as "any observable occurrence in a system or network," such as a server receiving a request for a web page, a user sending an e-mail message, or a firewall blocking an attempt to make a connection. The guide also defines *adverse* events as those with a "negative consequence, such as… unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data."

These events happen all the time. The latest *Dell Security Annual Threat Report*[2] found that malware attacks nearly doubled to reach up to 8.19 billion, and Symantec's *2016 Internet Security Threat Report*[3] revealed

that spear-phishing campaigns targeting employees increased 55%.

Category 2: Security incidents

A security or electronic incident is an event that violates an organization's security policies and procedures. Verizon's *2016 Data Breach Investigations Report*[4] defines an incident as a "security event that compromises the integrity, confidentiality or availability of an information asset."

Thus, a security incident is an event—such as a malware attack—that puts sensitive data at risk for unauthorized exposure. This could be any type of data, such as regulated financial or medical information or unregulated—yet crucial—information like intellectual property. Security incidents may also require you to report the incidents to your business clients per contractual obligations.

Category 3: Privacy incidents

According to the Centers for Medicare and Medicaid Services (CMS),[5] a privacy incident is an adverse event that happened as a result of violating CMS's privacy policies and procedures. The privacy incident must "pertain to the unauthorized use or disclosure" of regulated data, like personally identifiable information (PII) or protected health information (PHI). If the data involved in a security incident is regulated, the security incident is "upleveled" to a privacy incident. In other words, we could safely say that most electronic privacy incidents are security incidents, but not all security incidents are privacy incidents. Privacy incidents can also originate from non-electronic sources, such as mishandled documents or verbal or visual disclosure of PII or PHI. If you have contractual obligations to report privacy incidents to business clients, you must ensure timely notice to avoid breaching your agreements.

If you have contractual obligations to report privacy incidents to business clients, you must ensure timely notice to avoid breaching your agreements.

Category 4: Data breach

If a privacy incident meets specific legal definitions, per state and/or federal breach laws, then it is a data breach. Data breaches require notification to the affected individuals, regulatory agencies, and sometimes credit reporting agencies or the media. Additionally, contractual obligations require notice to business clients if the incident affected clients' employees or customers.

Only a small percentage of privacy incidents should escalate into data breaches if effective monitoring, reporting, and risk mitigation steps are taken when responding to the privacy incident. In order to avoid risk of over-notification or under-notification, organizations should document their incident risk assessment, notification decision, and timeline when the incident involves regulated data.

The Verizon *2016 Data Breach Investigations Report* showed confirmed data

loss in only about 3% of the 64,000-plus incidents reported. Despite the relatively low ratio of breaches to incidents, you're still obligated to determine if the incident is a breach. Organizations need to treat each privacy incident as a potential breach. The burden of proof is always on the organization to document and perform a multi-factor, incident risk assessment to demonstrate compliance or face penalties and corrective action plans from regulators.

Working together

Too often security events such as malware attacks stay in the domain of information security. But any time such an event violates policies and procedures and involves the potential exposure of data, it becomes an incident—and, possibly, a breach. It requires the expertise of privacy or compliance professionals to determine in which category these occurrences belong. Then, and only then, can you properly assess the risks of data exposure or loss to your customers and your organization and take the appropriate next steps. ✳

1. NIST: *Computer Security Incident Handling Guide*, 2012 is available at http://bit.ly/nistpubs
2. Dell: *2016 Dell Security Annual Threat Report* is available at http://bit.ly/sonicwall-dell
3. Symantec: *2016 Internet Security Threat Report* is available at http://bit.ly/st-report
4. Verizon: *2016 Data Breach Investigations Report* is available at http://bit.ly/data-breach-veriz
5. CMS.gov: Privacy Data Breach. Available at http://bit.ly/data-cms

Mahmood Sher-Jan *(mahmood@radarfirst.com) is CEO at RADAR in Portland, OR.* www *www.radarfirst.com*