http://ARMAPittsburgh.org

What Could Have Saved Sony Even After the Breach: Information Governance

A Few Specific IG Steps that Sony - and All Major Organizations Should Be Doing

By Robert Smallwood, Institute for IG

Vast amounts of confidential information was released to the public as a result of the recent Sony Pictures data breach. But it didn't have to be so. There are steps Sony could have taken before the breach which would have saved them even after the successful breach. All their confidential information could have been protected by applying a new approach—even if hackers were successful in gaining access. It's called Information Governance (IG).

The data breach was massive: Not only were unreleased films exposed, but also strategic marketing plans, detailed internal cost models, industry salary comparisons, termination/severance information, confidential email messages, email addresses and passwords, and even personally identifiable information (PII), including the social security numbers, birthdates, salaries, and performance reviews of all 3,800+ employees.

The "Guardians of Peace" hackers aim was ostensibly (and perhaps it was simple misdirection) to stop the release of "The Interview," a satiric movie about the assassination of North Korea's dictator Kim Jong Un. Estimates state the damage to the company as being in the $100 million range.

They are way off. If calculable, ultimately, the damage will likely exceed $1B to Sony in lost revenue, I.T. security costs, cyber-insurance costs, missed opportunities, employee turnover and hiring, reputational ill will, and perhaps other areas that have not yet been identified. Imagine if they are breached again. Now imagine one more time. They'd be out of business. That is, if they do not apply IG throughout the enterprise.

The negative economic impact will go on for years. Because, for one, even though Sony will try to cover the costs of identity theft for its employees, that lingering liability will be out there for years and years for those people. Their personal information is out there for the world to see. Certainly the credit card companies, banks, and credit bureaus will assist in the mitigation effort, but people whose PII has been revealed publicly can't change their birth date and changing their social security number or even name will take months, and involve voluminous paperwork. Rogue organizations that did not participate in the cyber attack may attempt to capitalize on the breached personally identifiable information (PII) right away or once things have cooled down months or years later.

Also, Sony Pictures' competitors now have keen insights into Sony's internal operating cost models and business plans. So they will not only move to counter those plans, but also, Sony will have to change some of them to less optimal approaches, due to the exposure of their strategies. Further, Sony competitors will easily be able to poach talent by simply offering a more secure and new work environment. Sony recruitment efforts will be more costly, and they will incur hiring, onboarding and training costs they would not have if not for the data breach, and breach of employees' trust.

And there may be more breached information that hackers accessed and are selling on the black market or they have yet to release.

What could have saved Sony - *even after the breach? Information governance.*

IG is an emerging multidisciplinary field that has slowly formed over the last five years or so but matured and gained great traction in 2014. It draws primarily upon the fields of privacy, security, IT, law, and records management. Even after the successful cyberattack, proper IG controls and technologies would have kept confidential information secure. But beyond that, it would have mitigated the reputational damage that was suffered when key Sony executives were exposed disparaging the talents of major stars like Angelina Jolie, Adam Sandler, and others.

Just exactly what is IG, and how could it have helped?

IG is more than cybersecurity, which obviously failed in this case. Let's be realistic: perimeter security does not work well, and even such elaborate approaches as "defense in-depth," which uses concentric rings of security to protect the organization's information assets, is fallible. Any organization can be hacked, and the larger they are, often the easier it is. And cybersecurity does not protect against malicious insider attacks. IG does.

IG is "security, control and optimization of information." Or, a more detailed definition is, "policy-based control of information to meet legal, regulatory, risk and business demands." Key words in this operational definition are "policy," "control" and "risk."

In short, IG is not only security but also control, and that means knowing what data you have, where it resides, and protecting it, especially confidential information assets and PII. Control means controlling not just the information stored in systems, but *controlling information that gets in* to the systems, and then who has access to that information after the fact.

So, if Sony's email policy would have stated, in part, "No insults or personally disparaging information about our employees, suppliers, contractors, or potential business partners may be stated in email or other messaging services provided by the Company," and there were clear penalties for violation, including demotion, pay cuts, suspension, or termination, then executives would have been discouraged from making such statements in writing on the company's email messaging system.

Too bad they didn't have that policy in place. Too bad they didn't monitor and audit it. Too bad the CEO was asleep at the wheel and did not activate an IG initiative within the company. What he needs to do now—or his successor—is to establish a Chief IG Officer (CIGO) position. Because these responsibilities fall outside the CIO's traditional and typical role of keeping information systems and networks up and running. The CIGO must be savvy and trained in all the component disciplines that make up IG, which go far beyond IT. That is why this responsibility gap is not filled in most organizations—few professional possess this cross-functional skill set. Sure, the CIO is responsible for cybersecurity but not for which data enters the systems. That falls on business unit heads—sort of. That's why a CIGO with clear C-level authority is needed.

But Sony's CEO is not alone, as most large organizations are facing the same type of massive risks. Yet they continue to delay implementing an IG program, as it would require management time and budget money that can be claimed as profit in the current fiscal quarter if it is not invested in IG. Short-sighted. Unnecessary and avoidable risk. *Poor management.*

The Sony incident opens up a Pandora 's Box for managers and shareholders; future attacks and blackmail schemes will come, and other organizations will be hit. Only next time they may demand money, bitcoins, weapons, hostages, or changes in corporate (or even governmental) policy. Rogue attackers now know they can bring a large corporation to its knees. Large corporations with deep pockets who are focused on quarterly profits, and "kicking the can down the road" when it comes to implementing IG programs. Sony caved in pretty fast.

Encryption of PII would have helped, but how does a company find all instances of PII? By using file analysis, classification and remediation (FACR) software across all servers to locate it within the company, and then securing it with encryption. There are other security and masking techniques as well.

But what about the confidential marketing plans and financial information? These electronic documents could be secured using information rights management (IRM) software which secures the e-document upon creation, and throughout its lifecycle. So Sony's spreadsheets with detailed cost information would not have been able to be accessed, even if they were copied. IRM uses encryption but it goes far beyond and secures confidential information assets based on context, such as when certain data is accessed, and on which device. IRM requires authorization to open a confidential document each time, and if it finds an unauthorized user has copied the documents and is attempting to open them, it will immediately "virtually shred" them on that device. Completely and totally erasing all remnants of the confidential document.

If you don't think this breach threatens Sony Pictures' very existence, just imagine if Sony's next 10 or 20 films are illegally accessed and released to the public for free. They'd be nearly out of business. Same for the other studios. Or music companies. Certainly maintaining physical separation of their new intellectual property (IP) from their network is a first step. That is an IG step.

IG begins with evaluating risks, and devising countermeasures to mitigate those risks. Then policies must be developed across information platforms, including email, cloud, social, mobile, SharePoint and others, and certain IG-enabling security technologies applied.

IG could have saved Sony Pictures a lot of embarrassment and expense. Now they will pay economic and reputational risk costs for years as they attempt to clean up the mess. And they have made a nice business case for IG which will be studied in business schools in the coming decade.

We can see the impact of management's failure to address these obvious IG risks, as made quite clear with the revelations of the Sony Pictures breach.

Will your organization be next?

Sony Pictures Breach Timeline

Robert Smallwood is author of "Information Governance: Concepts, Strategies, and Best Practices" (Wiley, 2014), and Managing Director of the Institute for Information Governance, which can be found at www.IGTraining.com

https://www.igtraining.com/live-online-training.html