AvePoint®

Implementing a Best Practice Approach to Risk-Based Data Protection and Cybersecurity

Dana Simberkoff, Chief Compliance and Risk Officer, AvePoint

Today’s Data Repository Challenge

Businesses increasingly work to create collaborative environments within their organizations. They are tasked with looking for new and innovative ways to organize and manage content and knowledge to increase productivity and reduce costs. At the same time, organizations are responsible for collecting, creating, using, appropriately sharing, and protecting critically sensitive data. Because of this, central information repositories are often full of unprotected, sensitive information. This trend makes these environments a target for attack and cyber threat.

Data without controls can create operational, privacy, and security gaps that could put an organization at risk. It can create unintended consequences and increases the potential for inadvertent or unauthorized disclosure of sensitive information. Businesses must comply with not only transparency requirements under existing and new privacy legislation, but also with requirements for protection of personally identifiable information (PII) and management of operational security. Improper exposure of this data can create privacy, operational, and security gaps that could put assets at risk. As organizations develop infrastructure consolidation and cloud strategies, this creates additional challenges for balancing access to information that should be available and protection of information that should not be available.

The Changing Landscape of IT

The average person is now quite familiar with the concept of cybersecurity. Breaches appear on the nightly news and, as a consequence, people are more “security aware” today than they ever have been in the past. Not only is there a heightened awareness level among individuals, but also there is a change in the policy and regulatory landscape. Audits, 24/7 media coverage, and public scrutiny have changed the economics of risk and created a constant “impending event."

While we’ve seen an increase in external pressures to protect information from customers and regulators, technology has also enhanced significantly. Digital advancements and the rise of social media have introduced a more complex and rapidly evolving ecosystem that has generated far more data to manage and protect than ever before.

More applications and transactions happen over the web and the cloud is completely changing our notion of a perimeter around which we can build protective walls. At the same time, worker mobility is redefining the IT landscape, with personal employee devices and “shadow IT” becoming the new landscape for IT.

Five Realities of the New Cyber Landscape

So what does this mean to the economics of a security program? How can you protect everything against everyone? With the increase of cybersecurity risks and information breaches, it is imperative that compliance, governance, and cyber assurance solutions for all data repositories and collaboration systems are strongly established and sustained. This is the reality of the new cyber landscape:

1. **Most attackers have a goal to retrieve information they could not otherwise obtain.** While organizations have limited budgets when it comes to protection against hackers, they are unaware that simple steps can be taken to protect against these attackers – many of whom are simply scouring for weaker targets. If you take simple steps to make it harder for attackers to retrieve data from your organization, they will likely go somewhere else.

2. **Security is all about mitigating risk.** In the absence of metrics, we tend to focus on risks that are familiar or recent. Unfortunately, this means we are often reactive rather than proactive. The importance of understanding how data, people, and location weave together to create patterns across your business is imperative to a secure system. Only by understanding the data you hold can you effectively protect it.

3. **Most costly breaches come from simple failures rather than attacker ingenuity.** However, “bad guys” can be very creative if properly incentivized. With the proliferation of ransomware attacks and the increased value of PII and protected health information (PHI), businesses must work hard to make themselves unattractive targets to bad actors, but prepare in case of disaster.

4. **In the absence of security education or experienced people (employees, users, and customers), poor security decisions are often made with technology.** This means that systems need to be easy to use securely and difficult to use insecurely. Make it easier for your end users to do the right thing with your data. Specifically, create policies, rules, and IT controls that make common sense for your end users to do their jobs effectively with the systems and controls that you want them to use. At the end of the day, your employees will do what they need to do to get their job done. Join them in making it simple to use the systems you can control.

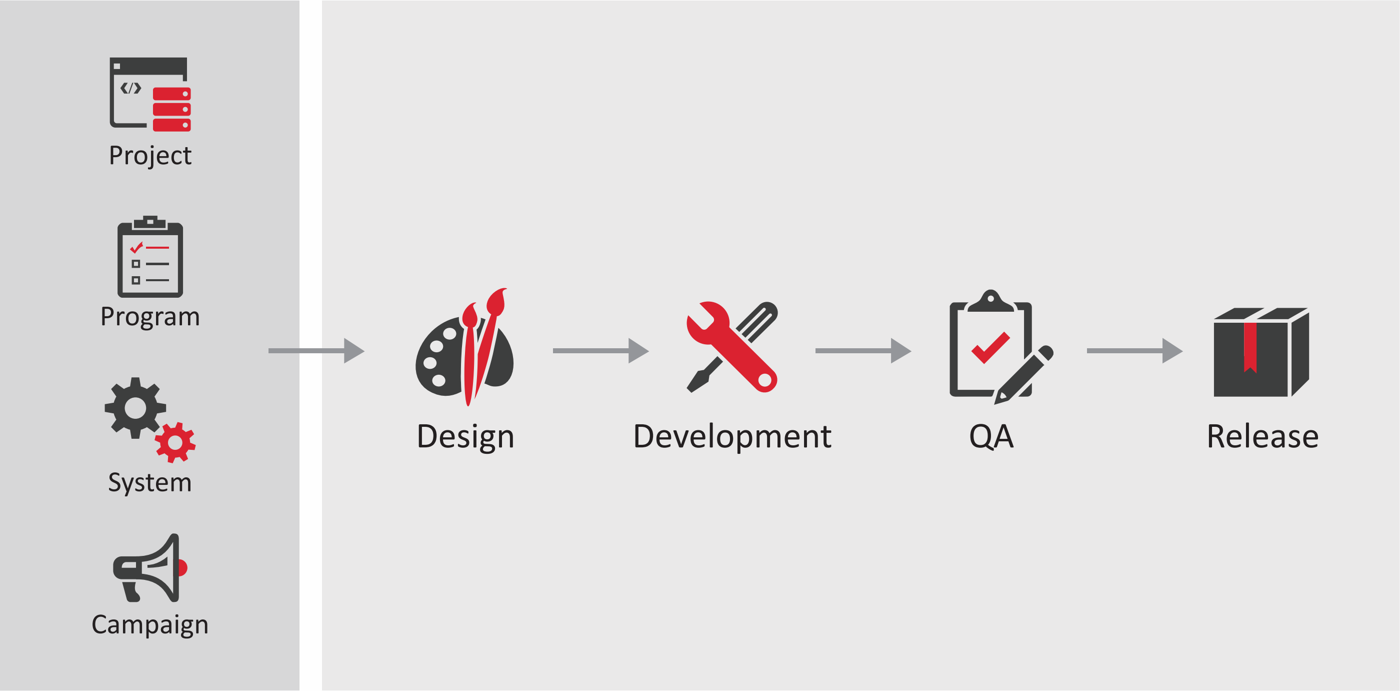
5. **Attackers don't usually get in by cracking some impenetrable control – they look for weak points, like trusting employees.** Many organizations make the mistake of focusing their data protection strategies on keeping the outsider out, but many breaches come from someone who is already inside. Either intentional or unintentional, insiders cause the greatest threat to your data protection program. Fortunately, several steps can be taken to alleviate the insider threat. You should trust your end users to appropriately identify and classify sensitive data, but verify that they are doing so in the correct way. Using a combined, or layered, approach to data classification can ensure that the policies, training, and tools you provide are properly understood and integrated into the day-to-day tasks of your work force.

Adopting a Risk-Based Approach

What do these trends ultimately mean for your organization? In order to have a holistic and effective data privacy and security program, you must understand that there is simply no such thing as perfect security. Instead, you must adopt a risk-based approach to implementing your data protection program.

Operationally, businesses should implement a strong mandate for security and privacy by design across all programs and assets. Traditionally, there has been a perception that privacy is where "IT goes to die" and that security "leads with no." Whether it's deserved or not, this is not an effective way to build a collaborative team.

Instead, it's important for security and privacy officers as well as legal counsel to take the steps to build privacy in as a foundational tenant of their development life cycles. Data protection must be embedded in every step of the organization's process – from the whiteboard stage of a new IT project, program, system or campaign, through the design, development, quality assurance, and release of the system.



This means that CISOs and CPOs must partner with their IT and program colleagues to gain key executive sponsorship and cooperation with their departments and programs. However, the reality is that security, privacy, and compliance offices are typically small parts of large organizations. These offices are tasked with ensuring compliance to many different standards for management of sensitive information internally and externally. They simply cannot be in every meeting in which a new IT system, program, or campaign is discussed. Instead, they can develop a framework that can be used by IT organizations to incorporate privacy best practices "by design and by default" within their line of programs and systems across the organization.

So how can this work operationally? By implementing a standardized and repeatable process with your colleagues in IT, you will be able to help provide advice, guidance, and review at every step of the process. Consider using automation to allow your colleagues to request a risk, security, and privacy impact assessment of the systems they are planning to build and deploy so you can provide them with a reasonable estimate and timeline. Your involvement early on will save your colleagues from having to make last minute design changes or decisions with the clock to launch ticking.

Creating a Solid Foundation with Your Privacy Impact Assessment

Speaking of impact assessments, if you are not doing privacy impact assessments (PIAs), or data protection impact assessments (DPIAs), there is no time like the present. As defined by the International Association of Privacy Professionals (IAPP), PIAs are a systematic process to "assess privacy risks to individuals in the collection, use and disclosure of their personal data. PIAs help identify privacy risks, foresee problems and bring forward solutions."

Many organizations already conduct PIAs as part of a statutory or regulatory obligation, and the European General Data Protection Regulation (GDPR) will also mandate PIAs. Impact assessments, like security assessments, provide a good foundation to assess the potential and ongoing risk of systems and data flows within them. That way, privacy and data security teams can recommend and monitor appropriate controls.

iapp

The IAPP exclusively distributes a free PIA tool available from AvePoint – the AvePoint Privacy Impact Assessment (APIA) system – that you can take advantage of today.

The New Era of Inter-Organizational Service Level Agreements

Through this kind of programmatic approach, and implementing security and privacy design automation, privacy program managers and data protection officers can then develop a service level agreement (SLA) with their colleagues in IT. What would this look like in practice? Consider the following high level approach:

1) **The program creates a new mandatory procedure that requires all new IT systems, programs, campaigns or processes to go through a quick and automated approval process before moving forward.** This would be required for all departments and applicable no matter where a program, concept, or idea is born. Using a tool like APIA (or any other registration system) the "sponsor" of the new system would register the idea and be prompted to go through a brief series of questions about the system. The questions might be about the goal of the project, lifecycle of the project, cost, or branding.

The key questions would be centered around whether or not this initiative would include critical assets, OpSec data, PII, or sensitive information of any kind. Based on the answer “yes” or “no,” the next steps would apply. If the answer is “no,” then for our purposes, no further action would be required other than perhaps to validate (again through automation) that no protected data was being used through the system. This is fairly simple to do through automated scanning, and can even be done through regular reviews and audits. If the answer was “yes,” then this program will involve protected data, and more steps need to be taken.

2) **Next, the privacy, data protection, and security teams can carry out an iterative review process and feedback loop – recommending appropriate procedures and technical controls to ensure that the sensitive data is protected.** Additionally, by having this information at the beginning of a project, rather than after it is already designed and “fully baked,” important data lifecycle management provisions can also be built in. This ensures data is retained only as long as necessary and is appropriately archived or destroyed at the end of a program – minimizing exposure and risk to the organization.

3) **In this model, privacy, data protection, and security check points can be built into the regular rhythm of this entire process, from the concept stage to end of life.** As a mandatory element of any new program (or review of an existing one) – privacy by design and by default now becomes the standard way of successful programs rather than an additional burden.

This standardized and repeatable process ensures that IT and the business understand and build in the appropriate privacy and security controls as a project begins rather than an add-on that is considered at the end of a project when it is about to go live. This enables security teams to help provide advice, guidance, and review at every step of the process. Teams should also consider using automation to allow your colleagues to request a PIA of the systems they are planning to build and deploy – so that the security team can provide them with a reasonable estimate and timeline.

Conclusion: Creating a Culture of Compliance

While a “culture of compliance” often starts with the legal and compliance team and ends with the CISO, it also needs to focus on a day in the life of your everyday employee. Security is everyone’s job. If you treat it as an afterthought, or leave it to the people in IT, or even to your CISO, then you have already failed. Every employee within your organization should understand that no one should care about the privacy of their own data more than they do, and they should work harder than anyone to protect it. Security should be as fundamental a part of employment agreements as anything else.

People often think of brakes on cars as being designed solely to stop cars – or slow them down. But, actually, with a feature like brakes in place, cars were safer to drive faster than ever before. Work very hard for your IT colleagues and program users to think of privacy and security controls in the same way. Rather than stopping the program from doing its job, put the proper controls in place to better realize the potential of the data you do have – so that you can achieve all of the program and business objectives you've set out to accomplish. Security by design builds those brakes into the system as part of the initial specification. When you are ready to roll a program off the assembly line and out onto the road, you'll drive away with full confidence in the data protection elements you've built in.

J. Trevor Hughes, President of the International Association of Privacy Professionals (IAPP) said, "Privacy is like a series of dams that we try to set up to limit the data we share as small data becomes big data." Technology and proper controls can ensure the flow of information is controlled, intentional, purposeful, and thoughtful rather than destructive to the organization. Trust is something that businesses must work to establish with customers every day. Once lost, it is very difficult to regain.

Dana Louise Simberkoff, JD, CIPP. Dana Louise Simberkoff is the Vice President, Risk Management and Compliance at AvePoint Inc. She is responsible for executive level consulting, research and analytical support on current and upcoming industry trends, technology, standards, best practices, concepts and solutions for risk management and compliance (Privacy, Information Security and Information Assurance, Data Governance, Compliance, etc.) Ms. Simberkoff is responsible for maintaining relationships with executive management and multiple constituencies, both internal and external to the corporation, providing guidance on product direction, technology enhancements, customer challenges and market opportunities.

Contact Us

Call: 201.793.1111
E-mail: sales@avepoint.com
Evaluate AvePoint Software for Free at:
www.AvePoint.com/download

AvePoint Corporate Headquarters

3 Second Street, 9th floor
Jersey City, NJ 07311

For US Government Organizations: Products can be purchased directly from AvePoint or through the GSA website at www.GSAadvantage.gov.

AvePoint®

www.AvePoint.com

AvePoint at a Glance

Founded in 2001, AvePoint helps more than 16,000 organizations and 6 million Office 365 users accelerate the migration, management, and protection of their Office 365 and SharePoint data.

Migration

Management

Protection

AvePoint, Inc. is headquartered and maintains its principal operational center in Jersey City, NJ, with approximately 1,500 employees across five continents.

- Australia
- Canada
- China
- France
- Germany
- Japan
- Netherlands
- Norway
- Singapore
- South Africa
- Sweden
- Switzerland
- United Kingdom
- United States

Microsoft Partner | Microsoft

Gold Application Development
Gold Cloud Platform
Gold Cloud Productivity
Gold Collaboration and Content

16,000
Customers

6 Million
Cloud Users

88
Countries

7
Continents

Deloitte
Technology Fast 500

Inc. Magazine
Hire Power Award
Inc. 500|5000

Ernst & Young
Entrepreneur of the Year

Windows IT Pro
Best SharePoint Product

Global, Live Support 24/7

Microsoft

100% Dedication to Microsoft Technologies

Microsoft Dynamics

Worldwide Public Sector Dynamics CRM GTM Partner

Microsoft Azure

Gold Azure Dual Credit Program

Microsoft Partner | 2017 Partner of the Year Winner Public Sector: Microsoft CityNext Award

2017 Microsoft Partner of the Year: Public Sector: Microsoft CityNext

Microsoft Partner of the Year 2016 Winner Technology for Good Citizenship Award

2016 Microsoft Partner of the Year: Technology for Good Citizenship

Microsoft Partner of the Year 2015 Winner Collaboration and Content

2015 Microsoft Partner of the Year: Collaboration and Content

Microsoft Partner 2014 Partner of the Year Winner Public Sector: Public Safety and National Security

2014 Microsoft Partner of the Year: Public Sector: Public Safety and National Security