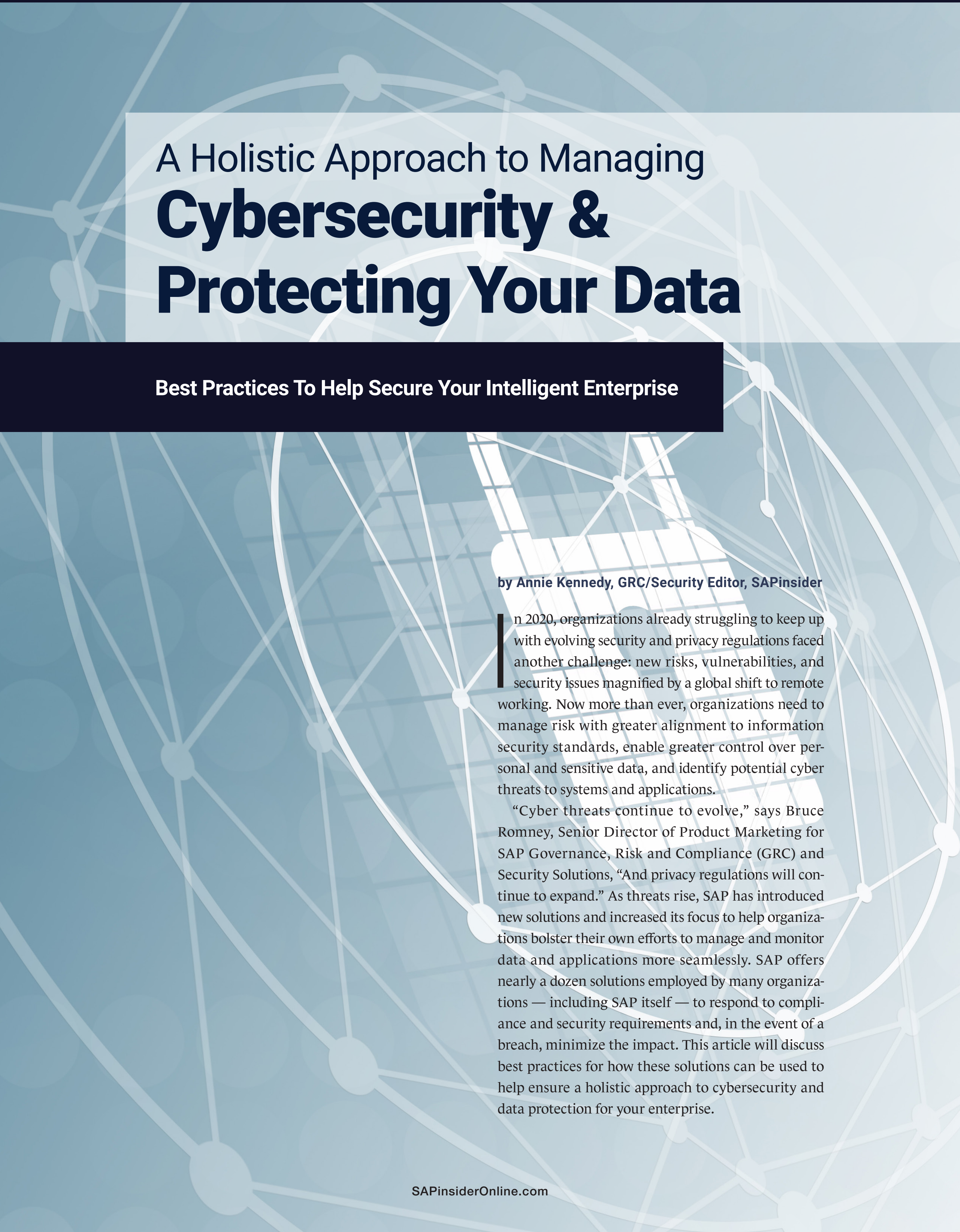

A Holistic Approach to Managing **Cybersecurity & Protecting Your Data**

Best Practices To Help Secure Your Intelligent Enterprise

by Annie Kennedy, GRC/Security Editor, SAPinsider

In 2020, organizations already struggling to keep up with evolving security and privacy regulations faced another challenge: new risks, vulnerabilities, and security issues magnified by a global shift to remote working. Now more than ever, organizations need to manage risk with greater alignment to information security standards, enable greater control over personal and sensitive data, and identify potential cyber threats to systems and applications.

"Cyber threats continue to evolve," says Bruce Romney, Senior Director of Product Marketing for SAP Governance, Risk and Compliance (GRC) and Security Solutions, "And privacy regulations will continue to expand." As threats rise, SAP has introduced new solutions and increased its focus to help organizations bolster their own efforts to manage and monitor data and applications more seamlessly. SAP offers nearly a dozen solutions employed by many organizations — including SAP itself — to respond to compliance and security requirements and, in the event of a breach, minimize the impact. This article will discuss best practices for how these solutions can be used to help ensure a holistic approach to cybersecurity and data protection for your enterprise.

Manage Risk with Good Cyber Hygiene: Educate and Integrate

For successful risk management, Scott Margolis, Managing Director for the Data Privacy and Protection Practice at Ernst & Young (EY), says that "companies should take an integrated approach to considering multiple perspectives by coordinating data privacy and protection, governance, and information security." For example, some of EY's clients have built data governance programs comprised of leadership representing security, privacy, risk, and information technology, meeting at least quarterly to look across the span of their business data and address the technological and procedural controls in place. In the same way that broader corporate objectives such as sustainability are being incorporated into entire organizations, the capabilities and broad aspects of GRC should be considered in a unified manner to create real-time visibility into risk.

Being able to identify who are the users in your SAP system is also crucial. Particularly when working in a remote environment where employees and partners could be logging in from all different internet protocol (IP) addresses, organizations should employ two-factor authentication to help combat threat actors. Criminals and other threat actors may succeed in using social engineering to convince an employee to share his or her credentials, but a second authentication could thwart them from getting further or doing damage. "We see things like multifactor application becoming more important, as well as monitoring users and what they're doing in the environment," says SAP Cybersecurity Solution Advisor Anne Marie Colombo.

She says that "knowing who did what inside your SAP system is often a blind spot for organizations." Solutions such as SAP Single Sign-On and SAP Enterprise Threat Detection can improve visibility and security within critical applications.

C-level and board members should also have data-driven insight so they can make decisions based on risks the organization is facing. Implementing SAP Digital Boardroom, which is built on SAP Analytics Cloud and can integrate with both SAP and non-SAP tools to pull information together at an aggregated and summary level, is one way to ensure that leadership can be proactive about managing risk, including cyber risk. According to Colombo, breaking down silos and documenting risk management by building up the risk register in SAP Risk Management can help companies facilitate implementation of risk management frameworks such as Control Objectives for Information and Related Technology (COBIT), National Institute of Standards and Technology (NIST), or Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Another important component to mitigating cyber risk is conducting regular monthly patch management for organizations of any size. SAP, a global company with more than 101,000 employees officed across 130 countries, applies monthly patches and uses Configuration Validation, a security template offered through Solution Manager, that enables SAP and its customers to determine whether the systems in their landscape are configured consistently and in accordance with industry requirements.

Finally, integration is key to ensure uniform risk management — both in business processes and governance as well as for software and tools that can integrate into the back end, particularly for organizations moving to SAP S/4HANA. "Integrated technology can support how well you respond to these risks. Having direct monitoring and governance around data and users within SAP S/4HANA can provide for more timely alerts, which can help thwart bad actors," says Romney.

Efficient Processes Drive Effective Automation

Many organizations are using automation to speed up manual tasks. While Margolis agrees that applying automation can add value, he emphasizes that its effectiveness is dependent on how efficient a company's processes are before they apply automation. "Applying automation to inefficient processes will only lead to streamlining inefficiencies or redundancies. Instead, build swim lane diagrams, run tabletop exercises to ensure your processes flow the way you expect them to, and work out the kinks on exception processes and variations on scenarios. Only after you've done that should you consider how to apply workflow automation and integration capabilities throughout other parts of the organization," he says.

Automating access to and monitoring digital assets through application programming interfaces (API) is especially important for companies that want to minimize risk in third-party management. Colombo

> Criminals and other threat actors may succeed in using social engineering to convince an employee to share his or her credentials, but a second authentication could thwart them from getting further or doing damage.

recommends that developer communities leverage SAP Cloud Platform API Management for embedded, enterprise-wide protection and safe asset sharing.

To address data protection and privacy for third parties, Margolis advises organizations to adopt standards and practices. Good examples include the regulatory requirements of the Office of the Comptroller of the Currency (OCC) or the Consumer Financial Protection Bureau (CFPB) and can serve as templates for your own governance. Additionally, the Cybersecurity Maturity Model Certification (CMMC) is offered by the Department of Defense (DoD) for business partners in the supply chain who deal with controlled unclassified information and require an additional level of cybersecurity.

Use Controls to Protect Your Data

It can be a challenge for companies to know what data they have, let alone where it lives. Many departments within an organization use separate programs and spreadsheets, meaning that data can live outside of a formal customer relationship management (CRM) system, for example. How can organizations securely track and protect all incoming and outgoing data?

Margolis suggests embedding controls into the design process to help protect data. "For example, companies can embed multifactor authentication, encryption of data at rest, and data disposal design and requirements after a period of time in order to respond to issues with early alerting," he says. Software firm BigID partnered with SAP to develop SAP Data Mapping and Protection by BigID, which uses machine learning to help organizations analyze and find data, understand the data flow, and document relevant information in a data privacy impact assessment to demonstrate that privacy controls are in place in the event of an audit.

To protect assets and comply with privacy laws, advises Colombo, organizations should minimize what users can access by segregating and protecting data. For instance, solution extensions from SAP partners such as NextLabs offer user interface (UI) masking and logging tools that promote data security and compliance by restricting access to any legally protected or business-critical data. SAP's UI logging package allows for recording and analyzing log data to monitor for atypical activity. By tracking what users saw when interfacing with the software, organizations can identify and shut down non-compliant activities and respond quickly. SAP also has a UI masking package which allows for configurable rules which determine which fields are visible to individual users.

Businesses should also be aware of data privacy regulations in order to be compliant and reduce risk. SAP Privacy Governance helps companies understand the requirements of regulations like the General Data Protection Regulation (GDPR) and manage the controls and actions needed to respond to these requirements. Managing data privacy impact assessments, data subject rights requests, and distribution of related policies are some of the elements of a privacy program supported by this solution. Colombo recommends including consent and understanding of data security as a component of any customer survey. "Explain at the start of the survey what type of data you are collecting and why to ensure respondents are aware and can give consent in order to continue participating," she says. "Upon completion of analyzing the results, be sure that you are safeguarding or disposing of the data collected."

As companies deploy SAP S/4HANA and move their primary stacks and systems into hyperscaler platforms such as Google Cloud, Microsoft Azure, or Amazon Web Services (AWS), they need to consider where the data resides geographically and under what regulations it falls, as well as monitor who can access it. Organizations need to ensure transparency into the different controls they use in reporting and in adhering to privacy laws that may differ among nations. SAP Data Custodian can help organizations manage services, specifying who can do what, on-premise or in the cloud. In addition, the SAP Data Custodian Key Management Service provides cryptography, encrypting and decrypting exchanged messages within an organization to serve as another barrier against threat actors. Cryptography can provide companies with another layer of confidentiality and authentication while assuring data integrity.

Anticipate Vulnerabilities and Have a Plan

Businesses need controls in place, along with real-time flagging and alerting, to monitor for vulnerabilities which are risk indicators in order to operate proactively. Automation applied to those controls can allow cross-functional teams to focus on improving security, accelerating cloud and SAP S/4HANA projects, and streamlining audit processes. The SAP-endorsed Onapsis Platform for Cybersecurity and Compliance can help organizations scan for vulnerabilities while automating testing, change, audit, and security processes, while SAP Enterprise Threat Detection (ETD) can continuously monitor the application layer to check for suspicious activity, such as someone trying to log into an application they don't have access to or log in at midnight on a Saturday to download gigabytes of data.

When it comes to financial transactions such as procure-to-pay, Romney advises organizations to utilize SAP Business Integrity Screening to monitor transactions and configuration settings in real time and in place (no need to extract or duplicate data) to help detect if a user — through acquired credentials — is generating potentially fraudulent transactions.

Even intrusion detection and controls may not be 100% effective. If a breach occurs, Margolis says, companies need to have an Incident Response Plan (IRP) in place that has been practiced, tested, and rehearsed. He advises companies to establish remote workforce policies and procedures and provide regular training to all employees on potential cyber and phishing attacks. Margolis suggests that organizations ask employees to keep a hard copy of their IRP in case ransomware makes online records inaccessible. Everyone should know who to contact — whether it's security, management, legal, or public relations — if an issue arises so it can be addressed immediately. "The threat actor only needs to be right once. We need to be right every time," Margolis says.

What Does This Mean for SAPinsiders?

In summary, SAPinsiders should consider taking the following steps to achieve a holistic approach to cybersecurity and data protection for the enterprise:

- **Anticipate and thwart threats proactively.** Create a cross-organizational governance structure to think ahead from a privacy perspective and minimize risk occurrence.
- **Follow good cyber hygiene practices.** Set up a regular patch process for your organization, and ensure that all employees are trained regularly on cybersecurity threats such as phishing and spear phishing.
- **Secure and protect applications and data.** Apply automation to your controls and processes to anticipate and mitigate threats, and leverage tools to monitor your SAP environment and provide real-time visibility into potential anomalies.
- **Plan ahead.** Ensure that everyone in your organization knows who to contact in case of an incident. ■