DocuSign®

Whitepaper

Security and Legal: An Essential Collaboration

How successful teams work together to ensure application security, threat detection and policy adherence

Introduction: Shared goals, complementary roles

Legal and security departments share the common goal of protecting an organization from harm. But, while both work to ensure security and compliance, the respective teams play distinct roles in achieving these goals. Through close collaboration and communication, each team can help the other optimize security and compliance throughout the organization.

For some organizations, legal develops security and/or data handling policies for the employees, to ensure proper handling of information. For other organizations, such policies may be developed by the security department in coordination with legal. These policies help define which information is sensitive, what constitutes authorized activity, and how to meet contractual, regulatory and internal compliance requirements. Legal and security often partner with human resources to keep employees informed about these policies.

Based on the requirements in these policies, security deploys tools and processes to build visibility and vigilance into the organization's data security ecosystem; this generally includes monitoring traffic and activity data and analyzing it for suspicious behavior. In the event of a security or other data incident, security will often involve the legal department to help evaluate the threat and determine actions to mitigate reputational, financial and other potential harm to the organization.

Successful collaboration between security and legal starts with well defined roles and responsibilities as well as proactive planning, before a data breach or incident occurs. Prior planning is essential because people rarely do their best work during a breach, and impromptu activity can further complicate an organization's response, including with regard to delivering breach notifications that may be required under applicable regulations.

Comprehensive plans should include day-to-day monitoring of user and third-party application activity, as well as detailed incident response procedures for addressing suspicious activity or breaches. As these plans are developed legal and security must consider external and internal threats as equally important. Though external threats generally receive more media attention, some threats to an organization may come from employee negligence, malfeasance or lack of training.

When evaluating third-party applications, legal and security must interact to ensure these tools are secure and compliant with applicable policies. This interaction, by necessity, begins with the evaluation and onboarding stage and continues through the implementation and maintenance stages.

A close, symbiotic relationship between legal and security helps keep the organization and its data safe and compliant. Together, these departments protect the organization by setting, communicating and enforcing effective data security and handling policies and procedures.

This white paper explores the interrelationship of corporate legal and security teams and highlights best practices for successful collaboration. Insights for this paper were gleaned from interviews with DocuSign legal and security executives along with experts from DLA Piper.

The challenge of preventing unauthorized activity

Security teams are tasked with detecting and containing a variety of threats, whether they originate from outside or inside the organization. While external threats are generally identified at the network level, increasingly sophisticated attacks like spear-phishing may be better addressed inside an application.

Internal threats and unauthorized activity can also be particularly challenging to detect because they can be intentional and malicious, or unintentional—stemming from negligent behavior or simple human error. In order to raise a red flag to address these threats, the security team must first define what constitutes suspicious or unauthorized activity.

Risks from insider threats

Breaches attributed to unauthorized activity such as negligent employee or contractor conduct can be just as damaging, if not more so, than malicious breaches. Regardless of the intent or source of the breach, the risk to an organization is equally serious.

The Ponemon Institute's 2020 Cost of a Data Breach Study found that:

- 7% of malicious breaches were caused by unauthorized insider activity
- 19% of malicious breaches were attributed to stolen or compromised credentials
- 23% of all breaches were attributed to human error such as negligent employee or contractor activity

These statistics suggest that threats often originate from within a company, and not just from external "bad actors." Also, the Ponemon study appears to reveal that even external threats can be attributed to—or exacerbated by—unauthorized employee activity.

7%
of malicious breaches were caused by unauthorized insider activity

19%
of malicious breaches were attributed to stolen or compromised credentials

23%
of all breaches were attributed to human error such as negligent employee or contractor activity

Source: The Ponemon Institute's 2020 Cost of Data Breach Study

---

"Monitoring activity and analyzing user behavior to watch for anomalies and potential intrusions are essential activities for protecting the company. If an employee violates a policy, it may be an innocent mistake or a signal of malicious activity. It's up to security teams to spot this activity and escalate to legal when needed."

Andrew Serwin
Partner, US Chair and Global Co-Chair, Data Protection, Privacy and Security, and Cybersecurity Practice
DLA Piper

Establishing data security and handling policies

While security teams are tasked with preventing, detecting and responding to threats, the legal team's responsibility is to align the organization to comply with internal policies, external regulations and contractual obligations it may have with third parties—regarding security and data handling controls. For this reason, and in certain cases, legal could be considered the architect of security policy.

How legal guides security policy

In establishing an effective security policy, legal may gauge the strengths and weaknesses of the organization, informed by direct input from security, to determine risk. Security and data handling policies combine obligations to comply with data privacy law, regulatory requirements, contractual commitments and applicable business operating procedures. First and foremost, policies may be developed to protect the company from liability. However, effective policies should also include comprehensive guidance on data security and prescriptive actions such as audit, reporting and incident response capabilities.

These policies set the tone for security priorities in an organization and help identify how sensitive or confidential information should be managed. This framework can also help security deploy resources strategically to protect the company, depending on where threats are most likely to originate.

For example, if a security policy identifies risk associated with data stored in a third-party application, security may devote additional resources to tracking activity in that application to detect unauthorized activity.

"Security and data handling policies are implemented to prevent risk exposure and help ensure compliance. We work closely with legal to understand the business risk associated with non-conformity with policies, and compliance risk in connection with regulations. Security is expected to monitor and safeguard data to a standard. And if unauthorized activity occurs, legal must also be informed to help assess the scale of the problem and the company's potential liability."

Niall McGrath
Senior Director of Security Operations
DocuSign

Enforcing data security policies

Security teams are an organization's subject matter experts regarding security, and thus are generally expected to take the necessary steps to protect an organization's data. From a technical standpoint, security teams monitor traffic and activity data. They also partner with the information technology (IT) department to establish permission levels that minimize the risk of sensitive information being compromised. Security must also anticipate threats, and work to address vulnerabilities that could be exploited by malicious actors.

IR plans and runbooks

Incident Response (IR) plans and runbooks are key assets as security teams organize their operations to address potential threats. An IR runbook consists of conditional responses which dictate actions in a step-by-step sequence. Responses Include a mixture of automatic technology-based actions and human decision-making elements, and typically include guidance on containing threats and sending notifications as part of the security operations process. Runbooks are usually authored by the company's chief information security officer (CISO) in consultation with the legal department, and should identify the extended set of key stakeholders across an organization who may be impacted by an incident. Documenting this information can help ensure alignment across an organization as to internal response activities beyond legal and security—as first and early responders—that may be required.

"Runbooks are prescriptive about communication and go/no-go points. The more detail security can provide to legal, the better the decisions legal can make about how to proceed."

Niall McGrath
Senior Director of Security Operations
DocuSign

A runbook establishes criteria for evaluating security incidents and provides a step-by-step guide prescribing actions to take at each stage. These criteria help teams evaluate security incidents to determine whether or not suspicious activity was authorized.

Runbooks also generally indicate when legal should be involved in the process, and legal works with the teams to evaluate specific go/no-go milestones and reporting requirements. Runbooks may also specify how and when security teams should update legal on the status of a security incident. Global runbooks can also help organizations standardize security operations across multiple locations, and adherence to runbook directives can lead to more consistent and effective security operations.

"Legal and security work together defining alerts. The security incident response plan and associated playbooks are written by the CISO and team with preset criteria. The plan details escalation criteria within security and indicates when legal, the Chief Privacy Officer (or Data Protection Officer), corporate communications, COO etc. will get involved."

Ronald Plesco
Partner, Privacy and Security, & Cybersecurity Practice
DLA Piper

Security as detective

One of security's primary responsibilities is to analyze activity data to detect suspicious behavior, and investigate that behavior to determine whether it was unauthorized. If security detects unauthorized activity that may indicate a breach, they will continue to investigate that activity and may take preliminary steps like closing an account to remediate the threat.

Once the threat has been addressed, security should collect all relevant information about the breach, and refer to the runbook to determine who should be informed, and when. More serious cases generally meet the criteria by default, for escalating to legal's attention.

"Legal works with security if there is a data handling incident. Security generally collects the data and investigates what happened, how, and when to determine the root cause. Legal provides support with respect to internal policies, regulatory compliance obligations and other contractual obligations that the organization may be subject to. The more information security can provide to legal earlier in the investigation about what happened to the data, the more we have a window into the black box of security and data protection. This puts us in the best position to help ensure continued compliance, determine how to mitigate liability and properly manage risk associated with the incident."

Cindy Rosser
Director of Product, IP and Regulatory Affairs
DocuSign

Once notified, legal reviews the incident in the context of a company's security and other applicable policies, relevant data protection laws and regulations, and contractual obligations. Security and legal then work together to follow the incident response plan, address the cause of the incident and prevent additional harm to the organization.

"Legal and security work together defining security strategies. If a difficult situation arises, security goes to their escalation process. The security incident response playbook (IR book) has preset criteria which are very clear. If this happens, then that happens."

Ronald Plesco
Partner, Privacy and Security, & Cybersecurity Practice
DLA Piper

How legal supports policy compliance

From legal's perspective, it's critical to ensure that the organization is compliant with internal company policies, governmental regulations and contractual obligations. Therefore well-designed compliance policies must address how organizations handle unauthorized activity as it relates to these obligations. This is critical because unauthorized activity may become an issue for legal, security, HR or other departments in an organization depending which department is responsible for the policy.

Compliance with data protection regulations

Compliance with GDPR, HIPAA, CCPA and other regulations underlie data security and other compliance-driven policies. For instance, CCPA imposes strict data privacy guidelines and even includes per-incident statutory damages for violations. Legal should work closely with security to ensure compliance with relevant data privacy laws to avoid compromising the security and protection of data governed by such laws. If a breach does occur, an effective and collaborative response can help mitigate the scope of the breach and reduce liability.

Security should also maintain sufficient controls to meet the minimum standards for data protection. Periodically, legal may recommend refinement of these controls to help ensure ongoing compliance, including notification requirements—to reduce potential liability for an organization.

Enforcing regulatory and compliance policies

Employees are expected to be informed of, and comply with an organization's security and data handling policies. While violating these standards can create legal issues, other teams such as HR, IT and security may also be involved. If a potential or actual violation is identified, legal must determine potential liability and what actions should be taken. In some cases, such violations may require reporting to company executives, regulatory agencies or even law enforcement.

"To help ensure ongoing compliance for our organization, we rely on mandatory training for all employees as well as operating playbooks which document and detail procedures and processes to support compliance. We regularly review and refine guidance around policies and controls to meet compliance obligations in an ever-evolving regulatory landscape."

Cindy Rosser
Director of Product, IP and Regulatory Affairs
DocuSign

Security and data handling incidents are usually detected by security teams, who oversee data-related activity across the organization. When unauthorized activity such as an apparent policy violation is detected or identified, security teams will generally investigate the incident and provide a root cause analysis to legal. The investigation may simply encompass the activity that led to the subject data incident, or in some cases, detailed information about where the unauthorized activity giving rise to the incident originated from.

With this information, legal departments can analyze the legal issues associated with the incident, including compliance concerns, incident risk level and potential liability for the organization.

Compliance and data security converge in third-party applications

Large organizations typically rely on third-party applications to perform critical business functions. These applications may serve a single team, or be deeply integrated across multiple business units in an organization. While legal is not solely responsible for the process of securing third-party applications, they will often partner closely with security to review and deploy new solutions as it relates to security and privacy. Specifically, legal will help determine whether their company's use of an application is compliant with internal standards, including compliance with regulatory requirements. Additionally, the security team may assess and evaluate whether sufficient controls are available through application features, to meet minimum information security requirements.

Evaluating third-party applications

Legal and security both review third-party applications to determine whether it can meet an organization's security and compliance requirements. Each team determines whether or not the application is compliant, and also takes into account the benefits of that application. These teams may consider compliance certifications, penetration tests, code reviews, feature audits, contractual flow-down obligations and other measures to evaluate the tool or service.

"When onboarding new applications from third-party vendors, legal may help evaluate compliance risk in connection with the use of such applications. Companies with a mature approach to compliance will often have established a process for assessing third-party vendors based on key compliance-related requirements. Legal, perhaps in conjunction with the CISO's office, may develop a risk profile for each vendor to help the organization as a whole determine whether to proceed with the use of that vendor's application."

Ronald Plesco
Partner, Privacy and Security, & Cybersecurity Practice
DLA Piper

A critical feature that organizations look for in third party applications is visibility into user and account activity. Security and legal teams may each benefit from activity visibility because it enables their organization to supplement existing compliance and security audit and monitoring capabilities. In particular, if a third-party application provides visibility into an organization's user and account activity, security teams may work with compliance and/or legal teams to identify risky or non-compliant activities for users of that application.

When preparing security response strategies implicating third-party applications used in production, legal can advise on recommended training and awareness efforts to mitigate unauthorized activity and educate users on best practices to avoid potential false-positives detected by the security team. For example, if an organization is concerned about employees transferring or deleting agreements in violation of their document retention policy, security could set up alerts to track account activity related to document downloads, transfers or deletions.

"Security needs to give legal teams visibility, like a camera to keep an eye on things inside a warehouse. While security can monitor the infosec landscape of an organization by tracking account activity and user authentication, they should also ideally be alerted if suspicious activity like large quantities of data are deleted or documents are sent to locations where the company has no offices, clients or suppliers. When a security incident does occur, security teams may then partner with legal to determine an appropriate response to meet compliance requirements."

Niall McGrath
Senior Director of Security Operations
DocuSign

Deploying third-party applications

If third-party applications meet an organization's security and compliance standards for deployment, legal may partner with security to help recommend activity and alert thresholds security operations should track and analyze. Further, If an organization is concerned with information being compromised in a particular application, security may need the ability to track things like downloads, logins or other activity that could lead to data being compromised in that application.

If a large proportion of sensitive or proprietary information is handled by multiple third-party applications, organizations may use security information and event management (SIEM) software to track activity across multiple applications simultaneously. These tools give security teams broad visibility into an organization's daily activity so they can investigate suspicious or anomalous behavior that may put the organization at risk.

For example, if an organization wants to use new software that will contain both proprietary and sensitive information, the application would be subject to a full vendor onboarding review process. Once the application is deployed, security may implement an operating plan and monitor application activity for unusual behavior using their SIEM system. If unusual activity is detected, security may refer to the relevant runbook to determine next steps.

Additionally, security can work with legal and IT to determine and establish appropriate access, admin and encryption protocols that comply with company policies and applicable regulations.

"When an organization is seeking to onboard a new application, diligence of the vendor is critical to helping an organization maintain compliance even through its use of that application. Perhaps infosec-related compliance controls mandate that the tool must log activity, have automated alerts or tightly integrate with our current systems via API. To what extent does the tool present risk to the organization? If the vendor fails to implement required controls, the tool will not pass muster with security requirements. This diligence review process is a critical step to help an organization meet its security and compliance obligations."

Cindy Rosser
Director of Product, IP and Regulatory Affairs
DocuSign

The benefits of effective collaboration between security and legal

Security takes on the day-to-day challenge of protecting an organization by detecting, investigating and responding to potential threats. Their team protects an organization by assessing internal and external threats, and addressing those threats as quickly as possible. Legal helps protect an organization by advising policy owners so appropriate teams are aware of security and regulatory policies. Legal teams are also a key function in an organization when it comes to enforcing company-wide adherence to both data security and compliance policies.

Documentation such as runbooks and data security policies are crucially important so security and legal are clear on what constitutes unauthorized activity, and what rises to the level of a breach. When an organization wants to use third-party applications that will be used to process or store sensitive or proprietary information, legal and security teams can work together to ensure the application meets both compliance and security standards.

Organizations rely on the close relationship between legal and security teams to ensure effective compliance and security safeguards are in place. Working together, security and legal can detect and address verified threats quickly, and take appropriate action. With regular communication and clear responsibilities, legal and security can establish a symbiotic working relationship to successfully protect and secure an organization's ecosystem.

"The industry is moving toward legal departments and CISO teams operationalizing a truly collaborative approach to application security, incident response and policy compliance."

Andrew Serwin
Partner, US Chair and Global Co-Chair, Data Protection, Privacy and Security, and Cybersecurity Practice
DLA Piper

Learn more about how to strengthen your security operations here:
docusign.com/products/monitor

DocuSign, Inc.
221 Main Street, Suite 1550
San Francisco, CA 94105

docusign.com

For more information
sales@docusign.com
+1-877-720-2040