Cross-Department Data Protection Checklist

Maximize Business Value by Evaluating Security Needs Across the Organization

Whether you're a global manufacturer, a small retail shop, a healthcare provider, a school, or a nonprofit organization, you have sensitive information that hackers can profit from, and that data can be found across every corner of your business.

When considering a solution for data protection, it's vital to keep the end users and their use cases in mind. This checklist will help you ensure your organization's most sensitive data remains protected, both in motion and at rest — even after it leaves your organization's network.

Departments That Need Data Protection

- **Executive Teams: Strategic, Confidential Communications.** Your executive teams are responsible for managing the enterprise, and this often includes highly sensitive data that needs to be protected at all costs. This can range from company strategy and forecasts to internal communications, as well as stakeholder or investor presentations, materials for the board of directors, and information related to mergers and acquisitions.

- **Information Technology and Support: Credentials, Passwords, and System Architecture Details.** Information technology underpins the entire organization's ability to operate. It also safeguards the company's passwords, access controls, system architecture, software (including patches), and customer account information.

- **Legal, Risk, and Compliance: Contract Details and Sensitive Documentation.** There's a reason the American Bar Association recommends encryption for client communications. Whether it results from user error or a targeted, malicious attack, a breach of sensitive legal data can rack up costly fines and fees, while damaging your company's reputation and eroding your clients' sense of trust. Additionally, much like the executive team, legal departments are entrusted with contract details and sensitive strategic information.

- **Finance: Internal Banking and Customer Payment Information.** This can include your internal accounting information, company credit cards and other sensitive financial documents, or customer financial data. If you process credit card transactions for customers, for example, those credit card numbers can be batch sold on the black market. Since hackers realize banks proactively monitor activity for suspicious transactions, they target massive stores of credit card information to make their efforts worthwhile.

- **Product, Innovation, and R&D: Intellectual Property and Trade Secrets.** Though harder to put a number on than physical goods, your intellectual property is one of your business's most valuable assets — and one that your competitors would love to get their hands on. Patents, product specifications and designs, research and development assets, proprietary sales and marketing plans, and other trade secrets fuel the success of your business. Letting them fall into the hands of corporate spies could give your competitors an opportunity to steal hard-fought market share and set you back years.

- **Sales and Marketing: Customer Lists and RFPs.** These teams may be externally facing, but they still manage sensitive data that needs to be protected. Market research, go-to-market plans for new products, customer lists, RFPs, and customer contract data are often managed by these departments, as well as shared internally. In 2021, USAID suffered a marketing system breach, where a hacker was able to send legitimate-looking phishing emails to its contact database via a third-party vendor.

- **Human Resources: Employee Financial and Personal Data.** Any business that houses sensitive personal data, like social security numbers, is a major draw to criminals looking to steal someone's identity. All those tax documents your new hires have to fill out? Those are potential cash grabs for someone with bad intentions and some hacking knowhow. And when salary and other privileged HR information ends up in the wrong hands, it creates employee relations crises and leadership challenges that are best avoided.

To ensure your business's data remains fully secure, it's critical to empower every employee with the ability to encrypt and safeguard their communications. Many organizations choose to extend data protection across their enterprise, including Virtru customer NEXT Insurance, a digitally focused leader in the insurance industry. Recently, NEXT increased its usage of Virtru and purchased licenses for every employee in the company.

"We want everyone to have the ability to protect the files they're sending," said Ram Avrahami, Head of Global IT and IS at NEXT Insurance. "At some point, everybody in the company will need to share something sensitive—maybe not daily, maybe not weekly—but eventually, they'll need to. Say for example, you want to send something that includes an attachment you want to protect, or you're sending an email with sensitive information that contains data loss prevention (DLP) keywords. We want to make it easy for these types of emails to be automatically encrypted."