

Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **May 2021**
Sponsored by **BlackFog**

What Decision Makers Can Do About Data Protection

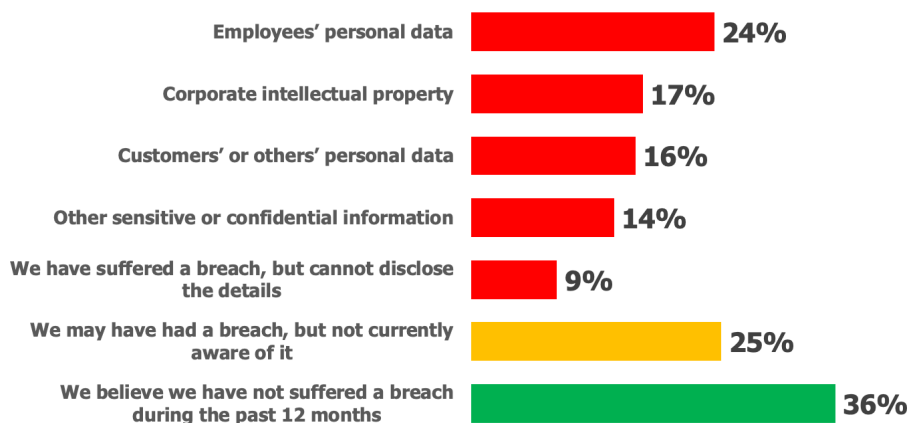
Executive Summary

No decision maker wants to be profiled in major media as being asleep at the wheel while a massive data breach, ransomware attack, or malicious insider incident unfolds at their organization. Careers rise and fall on a decision maker's ability to deftly guide an organization through the stormy seas of cyber threats, vulnerabilities, and security incidents, as does the reputation of the organization itself. Protecting data to ensure appropriate usage and avoid unauthorized or inappropriate usage is a major task for decision makers with responsibility for protecting the integrity of corporate data assets.

KEY TAKEAWAYS

- The term “data protection” encompasses a range of offensive and defensive plays to ensure that data is used by the right person for the right task at the right time – and nothing else. The growing number and variety of cyber threats and attacks makes this challenging to achieve.
- Organizations have been and are being impacted by cyber incidents including phishing attacks, ransomware (newly combined with data exfiltration), zero-day malware threats, mis-configuration of cloud services enabling massive data breaches, and account takeovers. Targeted attacks are especially pernicious and challenging to detect. Figure 1 illustrates just how serious this problem has become.

Figure 1
Types of Data That Have Been Breached
Percentage of Organizations



Source: Osterman Research, Inc.

- Employees are a frequent cause of data loss for organizations. So-called insider threats include inadvertent data loss from mistakes and negligence, as well as malicious data loss by disaffected employees undertaken due to a range of motivations. For organizations paying attention, however, the signs of upcoming data protection issues can be seen in advance.
- A growing panoply of privacy regulations around the world is contributing to the drive for heightened data protection approaches. GDPR, CCPA, HIPAA, PCI-DSS and others impose requirements on how personal and sensitive data is

The term “data protection” encompasses a range of offensive and defensive plays to ensure that data is used by the right person for the right task at the right time.

handled by organizations, and the principle of extra-territoriality redraws the lines of jurisdictional applicability.

- Shadow IT services, the use of personal devices, the adoption of a “cloud-first” or “cloud-only” strategy, and merger and acquisition activity, among others, represent a collection of other threats to data protection. Decision makers must evaluate the relevance and magnitude of these threats and develop appropriate counter-measures.
- Addressing the data protection challenge requires proactivity by decision makers. Engage the board, conduct a thorough audit across the organization, implement best practices, and use training and technology to strengthen defenses, elevate protections, and mitigate the major data protection risks facing your organization.

ABOUT THIS WHITE PAPER

This white paper is sponsored by BlackFog; information about the company is provided at the end of this paper.

What is “Data Protection”?

Protecting data encompasses a range of offensive and defensive plays to ensure that data is able to be used by the right person for the right task at the right time – and nothing else. While simple to state, the breadth of cyber threats and cyber-attacks that seek the opposite makes data protection a challenging task in the modern enterprise. Traditional tools, such as email, continue to be a key source of data leaks, and many organizations have inadequate processes and practices for archiving, backup, encryption, and data monitoring. It’s important to note that data protection focuses not only on unstructured data like email messages and files; but also structured data like Vehicle Identification Numbers, Social Security numbers, and the like.

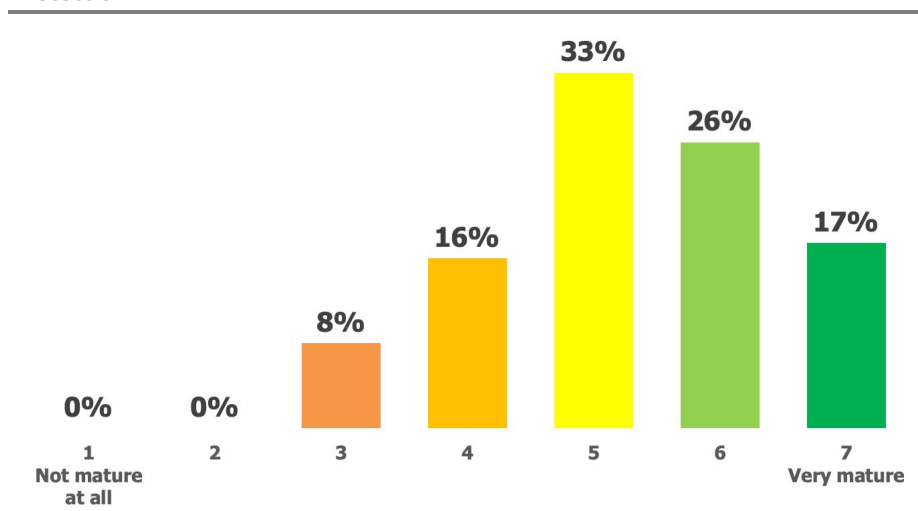
Data breaches are on the rise, with the first quarter of 2020 witnessing a higher number of breached records than the combined count of breached records for the first quarters of the previous seven years.ⁱ One mega-breach in the first quarter of 2020 exposed more than five billion records, and hardly a day goes by without yet another breach notification by an organization or cyber-attack alert against a country by a nation-state actor, and industries that have already been pegged as highly attacked are reporting ever-increasing attack activity.

Organizations are increasingly straddling two worlds, with different approaches to security. The first is the continuation of the on-premises model, where internal IT and security administrators have significant control over the systems and applications in use, and the cadence by which patches, updates and major versions are rolled out. The second, and relatively new, is a range of cloud services and applications where responsibility for security is shared between the organization and the cloud provider. While cloud service providers like Amazon Web Services, Microsoft Azure, and the Google Cloud Platform do a good, overall job of assuring the security of the cloud, these providers also make clear that the security of customer data in the cloud is their customers’ responsibility – the “shared responsibility” model. Few organizations are solely either on-premises or cloud, however, and straddle both simultaneously in a hybrid, and generally multi-cloud, model. Sensitive employee, customer and market data is increasingly flowing into a raft of cloud services.

Data breaches are on the rise, with the first quarter of 2020 witnessing a higher number of breached records than the combined count of breached records for the first quarters of the previous seven years.

Part of the problem is that many organizations' data protection posture is not what they would consider to be "mature", as shown in Figure 2. The work-from-home phenomenon driven by the global health pandemic in 2020 definitely has not helped. Cyber criminals have pivoted their malfeasance to prey on health fears through COVID-themed phishing attacks, steal new government funding from business owners through lookalike malicious websites, and leverage mass disruption to daily routines and security policies to compromise devices, systems and applications.

Figure 2
Maturity Level of Overall Organizational and Technical Approaches to Data Protection



Source: Osterman Research, Inc.

Data protection strategies, methods and approaches focus on protecting data from:

- Cyber security threats**
 Data breaches, phishing and spearphishing for credentials for unauthorized system access or fraudulent monetary transfers, ransomware that only encrypts data to undermine operations, ransomware that encrypts data and also publishes or auctions exfiltrated data to smear reputations and divulge intellectual property, and business email compromise are not abating.
- Inadvertent loss**
 Employees have authorized access to an organization's data, systems and applications, and honest mistakes during the course of daily activities result in inadvertent loss. Clicking on links in well-crafted, but malicious, emails; ignoring IT policies about copying or sharing data; or including customers' personal and account data in chat, files or email messages to the wrong recipient due to a type-ahead mis-click all result in data that is not protected as it should be. Loss can also result from inadequate processes, such as when an employee chooses to use a personal cloud storage account rather than the corporate sanctioned one because the latter is too complicated, resulting in data that's stored somewhere it shouldn't be and is now outside of the organization's control space.
- Malicious activities**
 While every employee has the potential to cause inadvertent loss through an

Honest mistakes during the course of daily activities result in inadvertent loss.

honest mistake or moment of negligence, a small number of employees deliberately attempt to create loss. Malicious employees use their knowledge of the organization's data to steal intellectual property as they leave for a new job with a competitor, maintain access to confidential project and customer data through a compromised account of a co-worker after they've been fired, or seek to complement their income by selling confidential data. Rogue database, system and IT administrators, likewise, can use their elevated privileges given with the intent of administration to access and download data they have no right to use. Some administrators have weaponized their engineering prowess to create a potent hacking capability that's turned against the organization or its customers.

- **Non-compliance with regulatory obligations**

Privacy is a global trend, and a growing set of regulatory mandates place significant obligations on organizations to protect data, obligations which carry severe financial penalties if ignored or not met. Europe's GDPR, California's CCPA, HIPAA for the healthcare industry in the United States, New York's NYDFS Cybersecurity Regulation for financial institutions operating in New York, and other existing and new data protection regulations around the world elevate the importance of data protection by design, introduce specific data breach identification and notification requirements, and transform penalties from being a mere slap on the wrist. New privacy regulations re-think the rules of jurisdiction, focusing on where the data subject is located rather than where the organization collecting or processing personal and sensitive data is based.

- **Other threats**

A range of other threats, including shadow IT, cloud applications, mergers and acquisitions, and the work-from-home phenomenon.

Cyber Security is Critical to Data Protection

An organization can have security without privacy, but cannot have privacy without security, and so cyber security is a critical component of data protection. Cyber security is critical to data protection and privacy, and the two are converging. In this section, we review the types of incidents that usually impact organizations, look at the areas of high concern for decision makers, and explore why targeted attacks are such a threat.

INCIDENTS THAT HAVE IMPACTED ORGANIZATIONS

Organizations have been impacted by several types of cyber incidents. Incident types that are commonly experienced are:

- **Phishing**

Phishing comes in several flavors, as alluded to already in this paper. General, mass-oriented attacks leverage the power of small percentages against very large numbers to catch out enough people to make the campaign worthwhile. Ensnaring even 0.01 percent of respondents in a million message campaign wins credentials for further attacks or system access to steal data. Spearphishing gives away the mass scale of phishing in preference for the specific targeting of people most likely to provide a fast route to a payout, while CEO fraud takes the idea in a related direction by impersonating the CEO or another high-ranking executive, again with a targeted attempt. Earlier in 2020, the bookkeeper at the real estate company of a high-profile investor was tricked into paying a US\$388,000 invoice for a real estate renovation to a bank

An organization can have security without privacy, but cannot have privacy without security, and so cyber security is a critical component of data protection.

account in Asia.ⁱⁱ When the bookkeeper initially queried the invoice, a detailed response and explanation was sent back by the cyber-criminal, a common technique to increase the likelihood of payment. People are much more likely to engage with a customized spearphishing or CEO fraud message than a general-purpose phishing one, simply because they recognize the name and role of the apparent sender.

- **Ransomware**

Cyber-attacks that disable access to systems and data through encryption continue to affect organizations across the world, although ransomware gangs are no longer content to only encrypt data and hope for a payout. Many ransomware operators have begun to exfiltrate the victim's data prior to encrypting it, and use either the threat of publication or the offer of auctioning it to the highest bidder to increase the likelihood of a payout. Both approaches are devastating to the organization: the first signals the presence of a data breach to data protection authorities, and the second fuels corporate espionage. Three ransomware attacks in recent weeks have included Hondaⁱⁱⁱ (which also impacted production of vehicles and motorcycles because the firm had to check if its quality control systems had been compromised), Conduent^{iv} (a large IT services company who had one gigabyte of data stolen in the attack), and the City of Florence in Alabama^v (after the IT manager fell for a phishing email apparently about a delivery by DHL).

- **Zero-Day Malware Threats**

Zero-day attacks attempt to take advantage of a weakness or vulnerability in the user's operating system, application or system to gain immediate control of the system, install unwanted software for stealing keystrokes or data over time, or gaining elevated privileges for future attacks. Zero-day attacks are timed to hit the market before the vendor in question has been able to release a patch to prevent the newly identified vulnerability from being exploited. Zero-day attacks are often carried out against commonly used systems, with Microsoft Windows and Office being high on the list.

- **Cloud Misconfiguration**

Cloud services require configuration and setup for each organization, and if either the IT administrator at the cloud service provider or the internal IT administrator at the organization makes a mistake during the configuration process, sensitive data is available for access by unauthorized people. In the case of the breach of more than 100 million records from Capital One,^{vi} the mis-configuration was on Amazon's side, where the web application firewall protecting the S3 buckets being used by Capital One was not set up correctly. An ex-Amazon engineer wrote custom scanning software to seek out mis-configured firewalls on S3 buckets, and stole data from Capital One and more than 30 other organizations.

- **Supply Chain Vulnerabilities**

Vulnerabilities in the IT environments of business partners, vendors and customers can introduce detrimental effects to an organization's infrastructure. The rise of outsourcing and offshoring has created ever increasing intertwinement of systems and applications, and weaknesses in the IT infrastructures of such third-parties can flow back to an organization. A simple example is a phishing attack against a third-party vendor that leads to credential loss and business email compromise on their end, and then misappropriated funds for others in the ecosystem. Bank of America had to

Vulnerabilities in the IT environments of business partners, vendors and customers can introduce detrimental effects to an organization's infrastructure.

issue a data breach notification to some of its customers in April 2020 due to a vulnerability in a system belonging to the U.S. Small Business Administration which it was required to use.^{vii} During 2019, an IT firm in Israel exposed customer data belonging to organizations in the United States and Canada due to insufficient security setting on its storage services.^{viii}

- **Account Takeovers**

Organizations face two types of account takeovers: of employees, and of customers. Credential theft from employees enables unauthorized access to email accounts (for stealing data or creating false email messages), customer databases, and ongoing fraud. Credential theft can be perpetuated by internal actors or malicious externals, the latter of which usually happens through phishing messages that lead to falsified websites. Allen & Hoshall, an engineering firm, suffered the consequences of an employee stealing the access credentials of a colleague.^{ix} Jason Needham, the thief, left Allen & Hoshall to start a rival engineering company, but continued to access Allen & Hoshall's data with the stolen credentials to then steal project proposal, engineering plans, and financial documents which he used in response to the same customer opportunities. When it's an account takeover of a customer, on the other hand, they more often lose access to their bank account or an ecommerce account, resulting in theft of money from their account, or products being ordered for delivery to a different address.

- **Sensitive Data in Documents**

Sensitive data is often stored in carefully protected systems with access controls and restrictions on usage. However, once data is exported from these systems – sometimes for valid business uses such as customer segmentation or powering a marketing campaign – it's easy to lose control over the data. Sending sensitive data in email messages or as attachments results in the proliferation of where sensitive data is stored, thus increasing the threat scape if an email account or cloud storage account is compromised. Databases and business intelligence analysts have access into data lakes and analytics platforms to sensitive customer data that is in the clear.

- **Other Issues**

Domain spoofing, brand hijacking, mixed threats (such as PDFs with malicious URLs inside), and password-protected attachments, among others, reflect other types of attacks or attributes that are used in the types of attacks we have already profiled above. When the attack relies on social engineering to gain a foothold, the fewer disparate or unexpected signals the better. Using the attributes of domain spoofing and brand hijacking in attacks, for example, take point people to fake login pages for Microsoft Office 365 or Google G Suite from a phishing message, warn a customer that their expected delivery from Amazon has been held up, send malicious emails from high-reputation IP addresses, or leverage a weaponized copy of a website for a well-known brand with a lookalike domain name and malicious downloads.

Organizations face two types of account takeovers: of employees, and of customers.

AREAS OF HIGH CONCERN FOR DECISION MAKERS

Decision makers often express high concern in the following areas:

- Phishing campaigns that attempt to wrangle credentials, system access, and data from unsuspecting employees and executives. Phishing campaigns are becoming increasingly sophisticated, and detection algorithms frequently miss

new campaigns thus delivering weaponized messages directly to the target's inbox.

- Shortages of cyber security talent to create robust defenses against new and emerging threats. IT administrators with well-honed security skills command premium packages in the market, and deeper-pocketed organizations can scoop the best.
- The proliferation of IT solutions and vendors to manage adds high cost, and high complexity, leading to interest in data security portfolio solutions addressing multiple areas, and architectural approaches to simplify, increased awareness of need to focus protection on the data itself. This is defense-in-depth to the data field level.
- Various types of malicious messages that infiltrate common communication systems, such as email, to deliver infected attachments, route CEO fraud messages, or provide a link to a ransomware download.

ON TARGETED ATTACKS

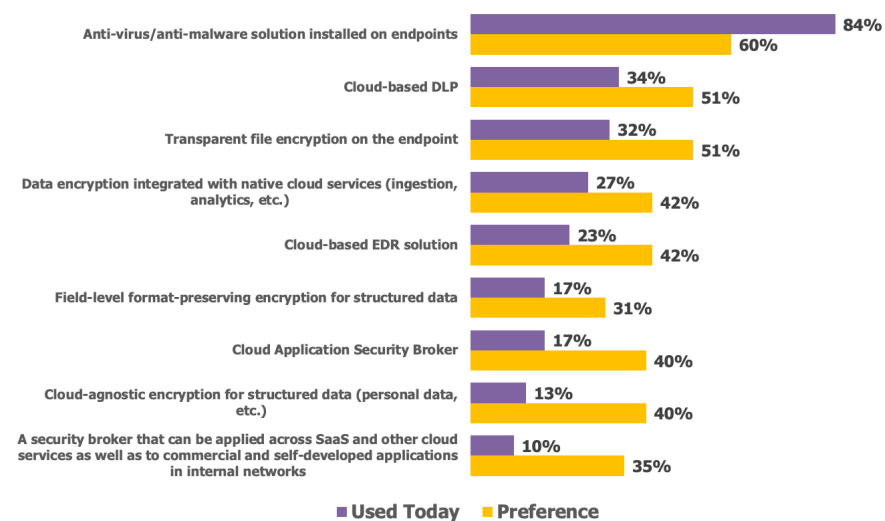
Targeted attacks pose a significant challenge in protecting data. As compared to general-purpose attacks that use general approaches and massive volumes with the intent of catching anyone (and anyone is fine, so long as someone is caught in the wide net), targeted attacks are more carefully crafted to ensnare a single individual or group. Cybercriminals create targeted attacks because they believe the likelihood and quantum of financial reward is higher than with general-purpose attacks, or in some cases, to prove a moral or political point. Primary targets usually have the direct fiscal authority to transfer funds, purchase something, or order an invoice to be paid under urgency. They also usually have high levels of access to sensitive data and systems. This includes CEOs, CFOs, partners, accounting staff, legal counsel, and real estate professionals, among others, with spearphishing attacks, credential theft, and unauthorized mailbox or system access prime vectors of attack.

Targeted attacks are challenging to detect for several reasons. First, because they rely on social engineering tricks and masquerade rather than code to perpetuate fraudulent activity, analyzing messages for code-based signals of wrongdoing turns up empty. There's no malware to detect, no URLs to scan for malicious behavior, and no rigged attachments. Second, the volume of messages is minuscule – potentially only one or two – hence the ability to act on widespread reports of spam or malicious intent from general-purpose attack campaigns is not available. Third, if normal channels of communication are compromised, such as email as a consequence of a phishing attack that netted credentials, without either party being aware, the attacker can insert new messages in a current stream of conversation requesting a new monetary transaction, or a changed bank account number for an upcoming payment. He or she can then quietly cover their tracks by deleting their messages and re-routing future replies out of the inbox into a subfolder to enable surreptitious interactions.

Part of the concern about protecting data from security threats is that there is a disconnect between the security solutions that are in use today versus what data protection decision makers and influencers would like to be using. As shown in Figure 3, many organizations are underutilizing tools that they would prefer to use, and overusing tools that do not provide adequate protection for their sensitive data assets.

Targeted attacks pose a significant challenge in protecting data.

Figure 3
Current and Preferred Tools in the Corporate Security Infrastructures



Source: Osterman Research, Inc.

Protecting Against Data Loss by Employees

Data protection includes the responsibility to protect against both accidental, inadvertent loss by employees, as well as loss incurred with malicious intent.

The inadvertent loss of corporate data is an everyday threat. Confidential and sensitive data can be lost when an employee stores corporate data on a personal device, home computer, or USB stick without appropriate protections in place. A lost phone that doesn't have a lock screen code, dropped USB stick, or home computer accessed by a visitor or other family member all result in the same outcome of loss. Many types of information are confidential and sensitive, including intellectual property (e.g., product research and design documents), lists of customers and their historical revenue numbers and current opportunities, personal information on people (including identity data, health data, and payment methods), price lists and discount sheets, sales data in aggregate or broken down by region or product line, and key contacts with phone numbers, email addresses, and reporting lines. Such data can be used to commit wrongdoing in a myriad of ways, including informing the design of spearphishing campaigns.

Data loss caused by malicious employees are less common than cases of inadvertent loss, but are frequently of greater negative impact to an organization. Motivations generally fall into one of several categories:

- Anger at being laid off or otherwise involuntarily terminated, resulting in a desire for revenge or retaliation. If the employee believes the organization still owes them a great debt for years of service, they may incline in the direction of freely taking that which is no longer being freely given, or unleashing an encryption program to prevent everyone else from doing their job.
- Anger at being passed over for promotion, or as a consequence of being reassigned to a different role that undervalues the skills they believe they

There is a disconnect between the security solutions that are in use today versus what data protection decision makers and influencers would like to be using.

possess. Tesla faced such an incident in 2018, after an employee wrote a program to exfiltrate data on Tesla's manufacturing systems and financial performance.^x The employee in question also installed his program on computers used by several other employees, in order to ensure ongoing, periodic exfiltration after he had left.

- The employee wants to gain an advantage in their new job or are working for a competitor. Exfiltrating intellectual property, customer lists, or product plans enables them to shine in their new work, and creates marketplace disadvantage for their previous employer. One ex-Google engineer was found to have taken 14,000 research documents on autonomous vehicles with him when he started his own autonomous vehicle company, which was subsequently acquired by Uber to bolster its competitive standing against Google.^{xi} The case of Jason Needham, above, is another example that would equally fit here.
- Trying to create additional income streams, either to fund a lavish lifestyle they can't otherwise afford on their normal salary, or in an attempt to pay off enormous gambling debts. Being willing to "do whatever it takes" to fund either direction can lead to stolen data, falsified invoices, and impersonation.

Unusual employee behavior can reveal potential or current data protection issues. Behavioral activity can be profiled to show patterns out of tolerance with normal baseline behavior for a given person or role, and the signs and signals acted on to prevent or stop malicious activity as soon as possible. A study by the Association of Certified Fraud Examiners in 2018 concluded that 85 percent of people behind fraud displayed behavioral red flags, and in the case of internal malicious cyber security activity, the red flags are available to be seen. Potential red flag behaviors include:

- Employees copying confidential and sensitive information to unsanctioned cloud services, USB drives, personal devices, personal file sync-and-share accounts, or sending such information to a personal email account. If there is no business reason for using these services or the use of these is against corporate policy, there's a red flag. The ex-Google engineer who left Google with intellectual property on autonomous vehicles was found after the fact to have copied 14,000 documents to his computer and then to an attached hard drive, and then to have deleted the documents from his computer to cover his tracks. The signals were there, but were not picked up until after he had left and the damage was underway.
- Significant changes in email volumes away from the individual's normal baseline pattern of email activity. A major spike of activity away from the baseline could indicate an employee distributing information he or she should not be sending out, or alternatively that the account has been compromised and an attacker is sending malicious emails internally or externally using the stolen credentials.
- Deleting a significant number of documents from their computer, network drive, or cloud storage account. Deleting a couple of new documents is likely to signal an attempt to correct an error, but deleting thousands or tens of thousands of documents from the past several years is more likely an abnormal event that signals an attempt to cause harm to the organization.

Data loss caused by malicious employees are less common than cases of inadvertent loss, but are frequently of greater negative impact to an organization.

- Access to corporate accounts or office facilities at unusual or weird times. Getting to the office early in the morning or staying late at night – particularly if current work demands do not require this of the entire team, or it is a new and abnormal pattern for the individual – could signal an attempt to use the quietness of a deserted office to create copies of confidential and sensitive data. Sometimes the employees who appear to be the most dedicated to their work by putting in extremely long hours and never taking a vacation are hiding nefarious and malicious activities.
- Opening lines of communication with competitors through corporate email, Skype, instant messaging or other services. If the organization has no business relationship with such competitors, and the individual involved is not charged with creating such relationships, then all such types of communication are suspect signals of an employee about to leave the organization, and perhaps to commit fraud while doing so. While employees should be free to interact with competitors if they are seeking a new role, communicating via corporate services to do so is inappropriate. Sending of corporate documents containing confidential, secret and sensitive information to competitors is a massive red flag.
- Accessing information that is not required in the normal course of work for an individual. Even if an organization embraces the approach of making all information available to everyone – which is widely discouraged due to privacy and security concerns – when someone actually uses this right to access information they have no business need for, it's a red flag. Equally, when network shares and cloud services are locked down to prevent unauthorized access, repeated attempts to access these content repositories by an individual should register as a red flag for review and intervention.

The ability to capture and correlate such signals in real-time provides the best opportunity for an organization to stop malicious activity in its tracks, or to take early action to protect itself from future loss.

Compliance Drives the Need for Data Protection

A growing panoply of privacy regulations is contributing to the drive for heightened data protection strategies and approaches. Privacy regulations are becoming increasingly common, such as:

- **GDPR**
The General Data Protection Regulation came into effect in late May 2018, offering a harmonized approach to data protection across all 28 member states of the European Union. It replaced a patchwork of varying data privacy directives across the union, and changed the basis of applicability from the location of the organization collecting or processing personal and sensitive data to the geography of the individual person on whom the data was being collected or processed. Now almost any entity that collects or processes data on data subjects in the European Union must abide by its data protection mandates and the expanded rights afforded to individuals (including rights of access, rectification, erasure and limitation of usage, among others).

A growing panoply of privacy regulations is contributing to the drive for heightened data protection strategies and approaches.

- **CCPA/CPRA**

The California Consumer Privacy Act and upcoming California Privacy Rights Act regulate the collection and usage of the personal data of California residents, copying the jurisdictional approach of GDPR in its applicability to organizations. CCPA came into effect in early 2020. As with GDPR, CCPA affords an array of rights to residents, including the right to be informed (of the types of personal data an organization holds on them and why), rights of deletion, right of transfer, and the right to opt out of the sale of their personal information.

- **HIPAA**

The Health Insurance Portability and Accountability Act of 1996, along with subsequent updates in the HITECH Act and HIPAA Omnibus Rule impose data protection requirements on health information and the organizations which handle, process and transmit it. HIPAA rules cover data privacy to protect health information from internal and external risks, security (including administrative, physical and technical safeguards), and breach notification. Penalties for violations are significant.

- **Financial Services**

Organizations in the financial services industry must comply with several regulations designed to capture and monitor electronic communication within the firm, ensure content is retained in an unalterable state, and ensure the privacy and security of the personal financial information of customers. Some state governments also have specific regulations for financial institutions operating within their jurisdiction, such as the Cybersecurity Regulation from the New York Department of Financial Services.

- **PCI-DSS**

The Payment Card Industry Data Security Standard governs how any firm offering payment options via credit and debit cards must protect and assure the security of payment data over time.

- **Other Privacy Regulations**

Countries around the world have taken inspiration from Europe's new data protection approach. Brazil introduced its General Data Privacy Law in 2018. India continues to argue its way through its Personal Data Protection Bill, with major revisions in 2018 and 2019. Australia amended its Privacy Act with requirements for mandatory data breach notification. Over 100 countries are moving in the direction of introducing similar regulations. Within the United States, the absence of a federal data protection approach has resulted in a patchwork of privacy regulations in different states, including Alabama, Colorado, Louisiana, New York, South Carolina and Vermont, among others.

Countries around the world have taken inspiration from Europe's new data protection approach.

PROTECTING "PERSONAL" DATA

"Personal" data is defined in several ways across varying regulations, but in general, refers to the information that alone or in aggregate can identify a specific individual. GDPR lists categories of personal and sensitive personal data including an email address, national ID number, photo, name, biometrics, sexual orientation, and IP address. It is equally concerned with protections on these specific data elements as well as the intended and combined use of them which can create sensitive personal data that wasn't directly evident before (e.g., profiling the name of an individual's partner to assess sexual orientation). CCPA focuses on similar data elements to GDPR, but also includes data elements that can be linked to a specific household or geographical address for profiling and segmentation. With the focus

on personal health information in HIPAA, the demographic data is covered along with past, current and expected health conditions, health care, and payments. Different regulations have different specifics, but there is a general commonality between them all.

The major change in new style data privacy regulations is the basis of applicability. Historically, data privacy and data protection regulations used the geography of the organization collecting or processing personal data as the basis of applicability. The new style regulations base applicability on the geographical location of the citizens or residents about whom personal and sensitive personal data is collected and processed, with no regard paid to where the organization doing so is located. Hence for an organization collecting or processing personal data on citizens of the Netherlands and residents in New York and California must equally comply with the mandates of Europe's GDPR, New York's SHIELD Act, and the CCPA.

WHAT IS DRIVING PRIVACY LEGISLATION?

The confluence of three major drivers are behind new and emerging privacy legislation:

- Consistency in rules to create a level playing field in the age of global ecommerce and global data collection technologies. For the European Union, for example, the fact that organizations outside the Union were not subject to the same responsibilities as those located within the Union under the previous data privacy approach created an unfair, tilted playing field in favor of non-European firms, which just doesn't make sense. GDPR harmonized the approach to data protection across the Union, while also imposing the same requirements on any organization collecting personal and sensitive data on people within the Union. GDPR and similar privacy regulations provide countries with the ability to hold the new style collectors of massive quantities of personal data – e.g., Google, Facebook, Twitter, and others – to account, even though they are not headquartered in their historic jurisdictional boundaries.
- The need for heightened security over personal and sensitive data, in light of massive accumulations of personal data in social media network companies ("surveillance capitalism"), cloud services, and huge corporations. Such data is being used to create systematic invasions of privacy, deny people their rights, and in some cases, interfere with democratic processes, e.g., the Brexit vote in the UK which was affected by the unauthorized and inappropriate usage of data by Facebook and Cambridge Analytica. Security is now an essential component of privacy legislation, including the requirement of a strong mix of organizational and technical measures, such as a Data Protection Officer to oversee data protection and security approaches (per GDPR), along with the recommendation to use encryption to decrease the negative effects of a data breach, among other impacts.
- Re-thinking jurisdictional applicability in the GDPR paved the way for the CCPA, with equal rules applying to organizations collecting and processing personal data on Californian residents regardless of geographical location. This principle of extra-territoriality enables countries and states to protect their people in an age of global commerce.

The growing tenor of privacy regulations will have significant impacts on corporate data protection approaches.

IMPACTS ON CORPORATE DATA PROTECTION

The growing tenor of privacy regulations will have significant impacts on corporate data protection approaches because there is a need to understand data – what it is, its sources, where it flows, how it is used, and if it needs to be used. This includes:

- The need to understand which data protection regulations apply, given the types of data being collected and processed from people across the world. Once these are understood, the decision has to be made whether to extend heightened data protection rights to every person or just those for whom the regulations demands it.
- The need to make provision for people to exercise their rights under applicable regulations, such as the right of access, deletion, and transfer (as appropriate). When a data subject requests access to their personal data, for example, a streamlined process is essential to ensure all relevant data is identified and made available within the timeframes required.
- Breach identification and breach notification requirements must be met, which requires monitoring, alerting and investigation systems to identify specifically what happened, and relationships with specialist cyber security and forensics firms to assist during breach incidents.
- An awareness of the heightened penalty regimes created by different regulations for non-compliance, insufficient safeguards, and data protection failures.
- The realization that hidden non-compliance with data protection regulations may be used against the firm by whistleblowers and aggrieved business partners.

Cyber actors, employees, and compliance regulations drive the need for data protection in the modern organization.

Protecting Data From Various Other Threats

Cyber actors, employees, and compliance regulations drive the need for data protection in the modern organization. Additional threats that contribute to the mandate for data protection include shadow IT, personal devices, cloud applications, merger and acquisition activity, and the recent sudden shift to work-from-home arrangements.

SHADOW IT

The use of shadow IT apps and cloud services results in confidential data being stored in systems with unknown security protections, the usage of apps that were never designed with business purposes in mind, and threats of unpatched and unidentified software vulnerabilities leading to data breaches. As employees embrace cloud applications beyond the list of corporate sanctioned services, inadvertent and malicious data leakage increases, along with unauthorized access to sensitive corporate data.

Shadow IT services that are not connected to the identity and authentication solution of the organization can also support malicious insider data theft. For example, revoking a user's identity on their departure or termination will prevent future access to services connected to the identity solution, but for non-connected

shadow IT services, no such prevention is possible. An ex-employee can continue to log in and access current and new data stored and shared through these services.

PERSONAL DEVICES

The use of personal mobile devices, laptops or desktops – at the office, while traveling, and most recently during new work-from-home arrangements – creates significant data protection problems for the organization. Such devices are generally outside of IT's security control scope, and the data on these devices cannot be tracked and monitored in the same way as for corporate devices. Equally, if devices are lost or stolen, the ability to remotely disable the device or securely erase all data is not usually possible, which opens the specter of a data breach and the financial and reputational damage that goes along with that. Personally-owned devices containing sensitive corporate data are also likely to slip through the net when an employee leaves the organization or is terminated.

CLOUD APPLICATIONS

Organizations are adopting a growing number of cloud applications, with many organizations emphasizing a 'cloud first' or 'cloud only' strategy. The proliferation of new cloud applications and multiple, disparate shared security models offered by a complex of vendors in a hybrid IT and multi-cloud environments creates a disjointed and uncertain security environment. The inability to detect where confidential, personal and sensitive information is being stored, accessed and shared from is a data protection failure, and if sharing and access settings are inappropriate or insufficient, cloud application can become a prime vector for data breaches.

MERGER AND ACQUISITION ACTIVITY

News of merger and acquisition activity usually heralds the significant opportunities awaiting the combined entity, but acquiring the IT infrastructure of another organization is rife with threat. Vulnerabilities across the infrastructure are unknown, previously as-yet-undetected data breaches are yet to come to light (and will hit the reputation of the acquiring organization), and new breaches may be in progress from angry insiders or attackers taking advantage of the uncertainty and hype of the acquisition.

SUDDEN SHIFT TO WORK-FROM-HOME

The forced embrace of the work-from-home phenomenon in response to shelter-in-place orders to slow the spread of COVID-19 in 2020 introduced its own bevy of threats, starting with insecure networks, unpatched applications, and the use of personal devices to access protected corporate data without the necessary access, encryption and usage protections in place. Corporate IT is blind to many of the threats lurking beyond their networks, and in the scramble to accommodate the new arrangements, security vulnerabilities and oversights that are yet to blow up will have been introduced.

It is clear that decision makers need to do something about data protection.

What Should Decision Makers Do?

It is clear that decision makers need to do something about data protection. The threats are too real and numerous to ignore, and the compliance mandates too costly to deal with in a half-hearted manner. In this section, we lay out a roadmap of activities for decision makers.

FOCUS ON DATA PROTECTION AT THE BOARD LEVEL

While the day-to-day operational aspects of data protection are the domain of every executive and employee, the board of directors is responsible for establishing the governance framework and strategic intent for data protection. The escalation of cyber threats, the range of possible inadvertent and malicious behaviors by employees, and the elevation of the regulatory environment have established data protection as a board level issue. The board must give data protection sufficient priority, funding, direction and urgency to equip the organization to meet its data protection responsibilities.

Directors, individually, must also understand that they are high value targets to cyber attackers. Directors have access to confidential business data, intellectual property, and strategic plans. Directors also offer cyber attackers the prospect of using their identities in business email compromise attacks, and thus protecting their identity, accounts, data and devices is an essential aspect of data protection.

Addressing data protection at the board level is not a one-time event. Regular briefings and reporting cycles should be instituted to ensure the board has a current awareness of the changing landscape of cyber security and data protection, and to check that each director is individually following through on their personal data protection mandates. Many organizations are required by mandates, such as the GDPR, to establish the role of Data Protection Officer. Others are establishing a new role in the Chief Data Officer.

CONDUCT A THOROUGH AUDIT ACROSS THE ORGANIZATION

Know the current state of data protection at your organization. Beginning with a thorough audit of security threats, current security tools, the types of sensitive data held across the organization, and more, is a standard and common recommendation (and even more so, a requirement in various regulations). It's the best place to start. Your audit should include an investigation into:

- **Security Infrastructure**

What current tools, services, and platforms make up your current security infrastructure? Which vendors are involved? For cloud services, are cloud providers meeting their requirements, and is there clarity on which security requirements the organization is responsible for? How current are the patch levels across servers, endpoints and applications? Is there a centralized identity service for granting access to applications? If there is one, how many services or applications are not connected to it? Developing a detailed checklist against which to review your security infrastructure is beyond the scope of this paper, but having one that you use regularly will assist greatly in developing a comprehensive approach to identifying new areas of weakness to address and current areas to strengthen.

- **Locate Sensitive Data**

What types of sensitive data are created, received, stored and processed across your organization? Where is it supposed to be held, and what protections are in place for those authoritative systems? Where is sensitive data not supposed to be, and how many instances can you find of sensitive data in the wrong place without appropriate protections in place? Are there particular people or groups who should have access to your sensitive data? How tight are the access controls for this data, and who has access who should not have access?

It is clear that decision makers need to do something about data protection.

- **Archiving and Backup Practices**

Review current practices for archiving and backup. What data is being archived? What data is being backed up? What data is excluded from either, and does that represent a risk-balanced decision or an oversight? Is there any data that must be retained by regulatory demand that is not sufficiently covered by current practices? Have there been any new systems or applications recently added to the organization without appropriate consideration given for archiving and/or backup? As well as understanding current practices, assess the current efficacy of these practices through a simulated restoration. If your organization suffered a ransomware attack that destroyed your operational capabilities, for example, would your current approach to archiving and backup provide the necessary safeguards to restore operations in a timely manner?

- **Employee Training Practices**

With the rise in cyber threats, cultivating an awareness of security and a healthy degree of caution among employees is essential. What is the current state of employee training practices for security at your organization? What proportion of employees have been trained in the past year, and who has missed out? It would be good to test the efficacy of your current training practices through simulated phishing attacks, social engineering attempts, and other evaluations; having trained all employees is a laudable standard, but the real test is how many can identify and ward off attacks in progress.

- **Employee Adherence to Corporate, Regulatory and Legal Policies**

Check how well employees are adhering to corporate, regulatory and legal policies. For example, are employees using personal cloud storage services in defiance of corporate policy? How many send sensitive data to their personal email account so they can continue working from home? Do employees have access to sensitive data that they no longer require for their job roles? A review of this nature will highlight areas of risk to address via a combination of process, training and technology.

While such an audit has to be done for a first time, conducting a periodic audit – at least once a year – to update the sense of efficacy of approach and make any required revisions to the plan is recommended.

IMPLEMENT BEST PRACTICES FOR USER BEHAVIOR

Make a determination on the best practices for user behavior in your organization for data protection. This is likely to include guidelines, policy making and technology-enablement to cover the use of corporate devices, personal devices, corporate data repositories, and more. Best practices to consider include:

- Corporate tools and devices should be used exclusively for corporate purposes, and employees should not use corporate devices to store, access and work with their own personal data. Settings for local encryption, authentication methods, and automated identification of sensitive data will elevate data protection on corporate devices, and if enforced before access is granted to corporate systems, greatly helps reduce various threats. It's important to identify solutions that can automate protection through the use of policy.
- Personal tools and devices have been frequently used by employees over the past decade, and if your organization will continue to support the use of personal devices, clarify the minimum standards required. This should cover, for example, operating systems supported, patch levels, and the presence and

With the rise in cyber threats, cultivating an awareness of security and a healthy degree of caution among employees is essential.

currency of anti-virus and anti-malware tools on the device. For employees accessing personal and sensitive personal data from personally-owned devices, one option to reduce data protection threats is to use virtual desktops where no data is ever stored locally on the device itself.

- Access to corporate data repositories should be carefully managed, using a mixture of general access permissions, conditional access rules to take account of risk-based attributes for each access session, and multi-factor authentication if the characteristics of the access attempt warrant it. Corporate data repositories should be used for corporate data only, and if backups are made, sufficient protections over backup devices enforced. Exporting data from corporate data repositories greatly increases the risk of inadvertent or malicious data usage, and should be dissuaded wherever possible through the use of secure integrations between systems rather than ad-hoc integrations using CSV exports.
- Limit employee access to sensitive data via need-to-know policies, segregation of duties, recertification of access rights, and the proactive removal of access rights when people leave the firm or change job roles. Administrator accounts should be used for administration purposes only, and should not also be intermingled with a user's day-to-day operational account for email and system access, otherwise a successful phishing attack against an administrator can cause devastating consequences through widespread system access and data breach. Recertifying access rights is a best practice because it gives the party responsible for a given data repository the regular opportunity to look over the list of people and groups who have access to the repository, and confirm whether such access rights continue to make sense. It's a good complement to well-managed identity and access management policies that proactively remove people from access lists when they leave the organization or move to another part of the firm.
- Identify solutions that encrypt data using techniques that maintain data format and referential integrity so that data can be used in its protected state without requiring decryption.
- Work-from-home policies and practices have suddenly taken on a much greater importance due to the global health pandemic in 2020 that continues to ravage many parts of the world. Users should know the risks of using personal devices if corporate devices are not available, and virtual desktop options should be considered to reduce the proliferation of sensitive data across unmanaged devices. Multi-factor authentication for corporate data repositories and systems should be increased, and other methods of secure access explored.

All users need to be trained on their data protection responsibilities, including executives.

TRAIN EXECUTIVES AND EMPLOYEES ALIKE

All users need to be trained on their data protection responsibilities, including executives. Senior executives, particularly, should be aware of the threats that can be unleashed against employees that impersonate their identities, and thus the greater care needed to avoid cyber security threats. Training should cover:

- How to recognize and deal with phishing, spearphishing and ransomware. Attacks of these types exhibit common signals, warning signs, and leverage current tricks of the trade. Knowing what they are helps with proactive identification (e.g., the iTunes gift card scam), and developing processes to verify abnormal requests with executives helps everyone keep organizational

data under protection. Alerting the IT department through streamlined processes of new attack possibilities also enables proactive removal of the threat from across the organization.

- Best practices for accessing, protecting, storing and deleting data. For example, personal and sensitive data should be stored only in corporate repositories, and the use of shadow IT services or sending such data to a personal email account or cloud storage service avoided. Even exporting data from corporate repositories for other purposes carries significant risk, and alternatives should be explored. Multi-factor authentication greatly helps with protecting data, and some types of multi-factor authentication tools – such as external hardware authenticators – are both faster and more secure than relying on second-factor codes sent by email or text message. Data subject to retention requirements should not be deleted.
- The privacy regulations under which the organization operates, and the employee's role in protecting sensitive and confidential data. Giving access to unauthorized individuals is a no. Copying confidential data to a personal device to take home is also a no. Taking lists of customers when an employee leaves the firm is a definite no. Clarity on role and expectation reduces any lingering uncertainty, and provides the organization with additional protections and avenues of response should an employee turn rogue.

IMPLEMENT THE RIGHT PROCESSES, TECHNOLOGIES AND TOOLS

The right processes and technologies complement the people and behavioral aspects of data protection we have discussed already. Building from the audit of current data protection approaches across your organization, processes and technologies are likely to be required in the following areas.

Cyber security tools to implement include:

- **Endpoint Protection**
Technologies that harden endpoint devices against security threats and attacks offer an essential line of defense in protecting the organization's data. All endpoints should have anti-virus and anti-malware tools as a baseline, along with endpoint behavioral monitoring to identify early compromise by malware or spyware. Technology enables endpoints to be controlled and managed by the organization, so that patch levels, application versions, and device health are routinely checked and verified before granting access to corporate data repositories. Non-compliance at the device level can indicate a compromised or unhealthy machine, which must first be rectified before access is granted. Additionally, tying specific devices to specific user identities greatly reduces the scope for an attacker to use stolen credentials to access corporate data from other devices. In addition, there are solutions available that enable the protection of sensitive data in files at the endpoint, with transparent file encryption, using policy to support productive collaboration but prevent unauthorized activity such as copying to flash drives, copy / paste, use of drop boxes, etc.
- **Server Protection**
Harden servers to reduce cyber security threats, including proactive vulnerability assessments and remediation of the operating system and applications (including virtual patching when necessary), continuous backup to enable rapid recovery in the case of a ransomware attack, and automatic

The right processes and technologies complement the people and behavioral aspects of data protection.

classification of sensitive and confidential data in order to apply appropriate protections. Servers should be also be in controlled spaces, in order to minimize inappropriate physical access to the machine. If it makes sense given normal access patterns, use IP address restrictions as well.

- **Gateways**

Since email is leveraged so frequently as a vector of attack, use secure email technologies to discover and remove email-borne threats, including phishing, malware and spam. Known threats that can be identified by signature-matching should be eliminated before they arrive to a user's inbox. Advanced threat protections address unknown, emerging and morphing threats that cannot be matched to a known signature, and rely on a variety of techniques to sanitize email traffic. Maximize the use of industry-standard email security protocols – such as SPF, DKIM and DMARC – to enforce protections on your email traffic for your benefit and the safeguarding of your customers and business partners.

- **Cloud Services**

There's no going back on the move to the cloud, and thus protecting the data and services made available through cloud services is essential. Use technology to track and assess access and usage, identify the presence of sensitive and confidential data (and automatically apply protections, such as access restrictions and/or encryption [format-preserving encryption, format-preserving hashing, tokenization, and data masking]), and verify that essential security configurations remain enforced. Cloud-agnostic data security solutions, such as Cloud Access Security Brokers (CASBs) and their derivatives, enable protections for personal and sensitive data in multiple clouds. One such derivative specializes in data protection for both cloud services and on-premises applications. This data protection gateway may co-exist with CASBs and specialize in doing the cryptographic heavy lifting to add strong, data-centric protection mechanisms that can be applied across SaaS and other cloud services, as well as to commercial and self-developed applications in internal networks.

- **Data Loss Protection (DLP)**

DLP technologies analyze content in motion and at rest to identify the presence of sensitive or confidential data. For example, if sensitive information is detected in an email attachment being sent to an external party, elevated protections can be automatically put in place, which range from blocking the transmission attempt, automatically encrypting the message and attachment, or double-checking with the original sender (or his or her manager) that sending such information externally is in alignment with business policies. Sensitive content located in files and documents on network file shares or in cloud services can be protected through restricted access lists or automatic encryption, for example, so that only people within the organization are able to read and edit with the content.

- **Data Exfiltration**

Modern attacks are predicated on the ability to communicate with third party servers to steal data. As a result, preventing attacks today requires a data exfiltration prevention solution that monitors, detects and blocks the unauthorized transmission of data in real-time. Unlike DLP, data exfiltration uses behavioral analysis to detect intent and operates on the endpoint of devices and can be used outside corporate networks. In addition, it does not

There's no going back on the move to the cloud, and thus protecting the data and services made available through cloud services is essential.

require the decryption of packets or breaking the SSL certificate chain. In a typical threat scenario an attacker will insert malware onto a network based device via malvertising or a phishing email. The malware will then crawl other network devices in search of valuable information before attempting to exfiltrate it. Because data routinely moves in and out of an organization, data exfiltration can closely resemble normal network traffic, meaning that data loss incidents can go unnoticed by IT staff until the damage has been done.

- **Field-Level Encryption**

Applications that use sensitive data – as well as databases, data lakes, analytic platforms and other repositories that use data in structured formats – benefit from field-level encryption to provide data-in-use protection for personal and high value data. Enforcing field-level encryption on sensitive “crown jewels” data assets enables business usage to drive value for the enterprise without compromising data privacy mandates.

- **Sensitive Data Discovery**

Many organizations have historical sensitive data stored in databases, applications, network file shares, email accounts, backup systems and endpoint devices without appropriate data protections in place. Even if an organization takes a perfect approach to data protection going forward, its historical data is still a potential landmine for compromise, data breach, and unauthorized access. Technologies that scan and evaluate all content across the organization for the presence of sensitive data highlight where added data protections are necessary. It makes visible the invisible, and provides directed guidance on what remains to be done.

MONITORING TECHNOLOGIES

Technologies that monitor the behavior of users, authentication patterns and cloud services, among others, provide early warnings of potentially malicious behavior. Consider monitoring technologies in the following areas:

- **Behavioral Baseline**

What is the standard pattern of behavior for a given user carrying out their job functions? Behavioral baselines profile system access, system activity, and times of day that particular activities are executed. Users beginning to diverge from these behavioral baselines may indicate that their account has been compromised or that they are pushing the boundaries on system access, both of which should be investigated post haste.

- **Authentication Patterns**

Monitoring the attributes of authentication patterns can provide early signals of password attacks, compromised accounts, or malicious activity by an employee. Repeated failed login attempts, login events from two different countries within minutes of each other, and login events at weird times of the day or night all say that something abnormal is happening, and having the insight into such happenings provides the data and urgency to act.

- **Usage and Compliance of Cloud Services**

As organizations make increased usage of cloud services, technologies that monitor access patterns, security configurations, data storage, new cloud services being adopted by employees without IT oversight, and vulnerabilities that haven't yet been patched support data protection mandates. Cloud Access Security Brokers (CASBs) provide a wide range of capabilities, and several

Technologies that scan and evaluate all content across the organization for the presence of sensitive data highlight where added data protections are necessary.

derivatives of this technology support focused monitoring of different types of cloud services. Integration of format-preserving encryption with native cloud services such for ingestion, storage, and data visualization enables persistent data protection, removes security gaps, and keeps control in the hands of the enterprise, wherever their data is.

- **Endpoint Monitoring**

Monitoring the behavior of the operating system and applications on an endpoint can provide early warning signals of a malware attack, data exfiltration attempt, or a ransomware attack in progress. Rapid identification along with automated isolation of affected endpoints protects the rest of the organization, and offers a streamlined approach for restoring a compromised machine to a healthy state.

ARCHIVING TECHNOLOGIES

Capturing important business records into an archiving solution enables elevated protections to be put in place on corporate data. Archiving technologies that are separate from day-to-day systems provide compliance officers, legal counsel, and security professionals with capabilities to restore forensically intact data, place content on legal hold, perform early case assessment on data drawn from multiple original repositories, and capture and manage records from an ever-changing roster of on-premises and cloud solutions.

EMPLOYEE TRAINING

Employee training on data protection approaches and requirements cultivates awareness, competence and a wider perspective on security practices. Training programs should cover the gamut of security awareness, heightened controls for sensitive and confidential information, and the compliance regulations under which the organization operates. A key part of employee training is ongoing testing to gauge the effectiveness of the material, and to identify where individuals and groups of employees require additional support.

OTHER TECHNOLOGIES

We have explored a range of essential technologies to improve cyber security above, but there are many others that will add value depending on the findings of your audit. Proactive vulnerability assessments of operating systems and applications, along with actual and virtual patching, reduce the likelihood that new vulnerabilities can be exploited by ransomware gangs or other cyber attackers.

There is no shortage of technologies available to strengthen cyber security readiness, but as with all risk mitigation approaches, these must be embraced in light of the magnitude and likelihood of the risk offset against the cost and effort of the available mitigation.

Summary

The mandate to protect data in the modern organization is wide-reaching, critical, and challenging. Data protection has to be more than words in an employee code of conduct manual, and cannot be left to fester while hoping for the best. Decision makers need to take informed and deliberate action to protect the data under their control against cyber security threats, inadvertent mistakes, malicious employees, and in order to comply with a growing range of new style data privacy and protection regulations. Look for portfolio solutions that help by providing complete,

The mandate to protect data in the modern organization is wide-reaching, critical, and challenging data.

reliable, adaptive, and automated approaches to navigate through the new world of data protection and privacy.

Sponsor of This White Paper

BlackFog is a global cybersecurity company that has pioneered on-device data exfiltration technology to protect companies from global security threats such as ransomware, spyware, malware, phishing, unauthorized data collection and profiling. Its software monitors enterprise compliance with global privacy regulations and prevents cyberattacks across all endpoints. BlackFog uses behavioral analysis to preemptively prevent hackers from exploiting vulnerabilities in enterprise security systems and data structures. BlackFog's preventative approach to security recognizes the limitations of existing perimeter defense techniques and neutralizes attacks before they happen at multiple points in their lifecycle. Trusted by corporations all over the world BlackFog is redefining modern cyber security practices.



www.blackfog.com

[@blackfogprivacy](https://twitter.com/blackfogprivacy)

sales@blackfog.com

© 2020-21 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

REFERENCES

- i Nick Forrester, *Q1 2020 Sees More Data Breaches Than Ever Before*, Security Brief Asia, May 2020, at <https://securitybrief.asia/story/q1-2020-sees-more-data-breaches-than-ever-before>
- ii Nicole Lyn Pesce, *'Shark Tank's' Barbara Corcoran Fell For This Very Common Phishing Scam - and it Cost Her Almost \$400,000*, MarketWatch, February 2020, at <https://www.marketwatch.com/story/shark-tanks-barbara-corcoran-fell-for-this-very-common-phishing-scam-and-it-cost-her-almost-400000-2020-02-27>
- iii *Honda Hit by Ransomware Attack*, IT News, June 2020, at <https://www.itnews.com.au/news/honda-hit-by-ransomware-attack-549064>
- iv Meera Narendra, *Maze Ransomware Strikes IT Services Firm*, PrivSec Report, June 2020, at <https://gdpr.report/news/2020/06/08/privacy-maze-ransomware-strikes-it-services-firm/>
- v Brian Krebs, *Florence, Ala. Hit By Ransomware 12 Days After Being Alerted by KrebsOnSecurity*, KrebsOnSecurity, June 2020, at <https://krebsonsecurity.com/2020/06/florence-ala-hit-by-ransomware-12-days-after-being-alerted-by-krebsonsecurity/>
- vi Greg Kumparak, *Capital One Hacked, Over 100 Million Customers Affected*, July 2019, at <https://techcrunch.com/2019/07/29/capital-one-hacked-over-100-million-customers-affected/>
- vii Caroline Hudson, *Bank of America Reveals Data Breach in PPP Application Process*, May 2020, at <https://www.bizjournals.com/charlotte/news/2020/05/26/bank-of-america-discloses-ppp-data-breach.html>
- viii Catalin Cimpanu, *Contractor's Server Exposes Data from Fortune 100 Companies: Ford, Netflix, TD Bank*, June 2019, at <https://www.zdnet.com/article/contractors-server-exposes-data-from-fortune-100-companies-ford-netflix-td-bank/>
- ix The United States Department of Justice, *Tennessee Man Sentenced for Unauthorized Access of Former Employer's Networks*, August 2017, at <https://www.justice.gov/opa/pr/tennessee-man-sentenced-unauthorized-access-former-employers-networks>
- x Lora Kolodny, *Tesla is Seeking \$167 Million in Damages from the Former Employee Elon Musk Accused of Sabotage*, CNBC, December 2018, at <https://www.cnbc.com/2018/12/11/tesla-seeks-167-million-in-damages-from-ex-employee-martin-tripp.html>
- xi Michael Liedtke, *Ex-Google Engineer Accused of Stealing Self-Driving Car Trade Secrets Before Joining Uber*, USA Today, August 2019, at <https://www.usatoday.com/story/tech/2019/08/27/google-uber-anthony-levandowski-stole-company-secrets-sold/2131755001/>