An Enterprise’s Guide to Data Security and Secure Communications
Your company has been built with hard work and dedication, and naturally, you want to protect it. Cyber attacks are becoming more rampant, with studies showing that someone somewhere is a victim of a cyber attack every 39 seconds. While data breaches are becoming more common, they can be detrimental to a company. The average data breach costs $3.92 million, and it takes companies an average of 191 days to even notice a breach. Damages from cyber crime are estimated to be up to $6 trillion annually by 2021.

The problem with cybersecurity is that some companies think that they don’t need it — until it’s too late. You may ignore the threat of hackers, but they won’t ignore you for long. It’s imperative that you keep your company protected and secure so that your business can thrive.

**Why You Should Invest in Data Security**

Is this spending on data security worth it? The short answer is “yes.”

Of the organizations surveyed by Cisco, more than 40% said they saw financial benefits at least twice that of what they spent on data security. Smaller companies with 250 to 499 employees saw a yearly benefit worth $1.8 million. For companies with 500 to 999 employees, that benefit rose to $2.3 million, and companies with 1,000 to 9,999 employees saw a total benefit of $2.9 million. The largest companies, with more than 10,000 employees, reaped $4.1 million in financial benefits from their investment in data security.

Comparing the financial benefits with the yearly investment results in an estimate of a company’s return on investment for data security. Almost half (47%) of the companies surveyed saw an ROI of more than 2 to 1, while a third broke even on their investment. Only 8% saw no measurable return on their investment.

The bottom line is this: For every $1 of investment in data security, the average company received $2.70 in tangible benefits. (Note that the rate of return did not vary much by company size; the ROI was similar for small, midsize, and large companies alike.)
Business Benefits from Data Security

In addition to the direct financial benefits from data security spending, companies reap a wealth of important business benefits. Cisco reports that more than 70% of the companies surveyed said they'd received significant business benefits from their investment in data security.

What kinds of business benefits did these companies experience? The following percentage of respondents noted significant benefits in these specific areas:

- Building loyalty and trust from customers, 74%
- Making the company more attractive to investors, 73%
- Achieving operational efficiency from data controls, 72%
- Enabling innovation and agility, 71%
- Mitigating losses from data breaches, 71%
- Reducing business delays, 67%

The benefits are many and significant, and they can't always be measured in direct financial terms. Consider them to be above and beyond the ROI resulting from ongoing data security spending.

Better Data Security Means Lower Costs from Breaches

The more effective the data security practiced by an organization, the less financial exposure due to data breaches. This results from both a decreased number of breaches and a lower cost incurred from each breach.

Cisco measured what they call data security accountability for each of the firms participating in the survey. This rating roughly corresponds to the number and types of data security measures put in place by each company.

On a scale of 1 to 5, a company with more data security accountability earns a higher score, as follows:

1.0: The organization has little data security in place.
2.0: The company is working on its data security and has made some progress.
3.0: The firm has made significant progress in its data security but still has a substantial way to go.
4.0: The organization has a majority of recommended data security measures in place.
5.0: The company has all or nearly all recommended security measures in place.

Based on data collected, those firms with the highest scores experienced the fewest data breaches. Of those firms with scores of 4.0 or lower, only 13% reported no data breaches in the previous year. For those companies with scores above 4.0, however, the record was twice as good — 28% experienced no data breaches.
Protecting Your Data: Best Practices

The benefits of protecting your company's data are obvious. Now it is important to know what your enterprise needs to do to protect your important data. Enterprises employ data encryption to protect valuable data from unauthorized access. To ensure the strongest protection against data breaches and theft, organizations must follow best practices in choosing which data to encrypt, how to encrypt it, and who has access to that data.

— Identify Valuable Data

A large organization may have sensitive data stored in multiple physical and virtual locations. It is necessary to take an inventory of where the most valuable data is located at all levels of the organization. This includes both data at rest and data in transit across the network. Once these locations are pinpointed, you need to prioritize the most valuable data assets and storage repositories. This will help you develop the best strategy for encoding the data.

— Protect Data at Rest

Data at rest includes all data stored on physical media, whether magnetic, optical, or solid-state devices. The most effective way to protect data at rest is through strong encryption controlled by cryptographic keys.

— Protect Data in Transit

Data in transit refers to data transferred between locations or components, typically over the network or to/from cloud storage. Data in transit is vulnerable to various types of attacks, including session hijacking and man-in-the-middle attacks, that can gain access to all manner of confidential data and communications. To protect data in transit, use SSL/TLS protocols, virtual private networks (VPNs), and end-to-end encryption.

— Choose an Appropriate Encryption Algorithm

There are multiple encryption algorithms in use today. Best practices dictate embracing state-of-the-art encryption that has been properly tested in real-world situations. Consider factors such as memory usage, encryption speed, and cost. You should also make sure the encryption you choose adheres to relevant international and industry standards, including those set by the National Institute of Standards and Technology (NIST).

— Manage Cryptographic Keys

Protecting your cryptographic keys is imperative to protecting your organization's sensitive data, especially any data stored in the cloud. The best secure containers, known as key vaults, help you maintain secure control of the keys used to encrypt and access your data. Key vaults also control and log access to any items stored within, such as certificates. Your organization's IT security staff should manage key permissions as necessary. Best practice is to grant access to groups, users, and applications at a specific scope, such as a resource group or subscription.
— Control Interface Access

IT staff should also control which users have access to what interfaces. Key vault access is controlled through the management plane and data plane interfaces. In most instances, a user, group, or application needs access to only one of these planes, not both, which increases the level of security.

— Store Certificates in Key Vaults

Another best practice is to use key vaults to store high-value certificates. If certificates are compromised, the security of an application or its data can also be compromised. Employing key management to certificate storage helps control who has access to each certificate.

— Ensure Key Vault Recovery

If a key vault is accidentally or purposefully deleted, the data stored within may be lost. IT staff should employ a management solution that lets you recover any deleted key vaults and objects.

— Practice Scalability

Your encrypted data security solution needs to be able to scale across all your data. It should also automatically adapt to any changes in your storage methods, especially including growth in the amount of data stored.

— Integrate with Cloud Systems

According to IDC's Data Age 2025 report, by the year 2025, 49% of all data will be stored in the cloud. Best practices ensure that data security and encryption are applied to all cloud-based data storage. Your security and encryption should work with your cloud storage provider and any applications that use cloud-based infrastructure.

— Use Secure Workstations to Access Data

All access to sensitive data and accounts should be limited to secure workstations. Using a workstation with privileged access minimizes the risk from phishing and other social engineering attacks that compromise user credentials to gain access to sensitive data.

— Enable Endpoint Protection

Any device that is used to access data presents a breach risk. This includes not only workstations and desktop computers but also notebooks, smartphones, tablets, and other devices. IT security staff should create and enforce strict security policies for all devices that touch your organization’s data.
Protecting Your Business Communications

Keeping your data safe is just the first step. One of the biggest threats to your company's data security is how your workforce communicates with each other. Successful collaboration means constant communication, and if you aren’t careful about how your employees communicate with each other, valuable information can be stolen in the process.

Email has previously been a standard for workplace communication, but due to security concerns, it is becoming more of a liability than an asset. Business Email Compromise (BEC) accounted for half of business losses due to cyber crime in 2019 — an estimated total of $1.77 billion.

To understand how to protect your company or organization from BEC, it is important to look at why these attacks are so successful. While there are differences in sophistication and scope, the equation for a successful business email compromise is reliant on two key variables:

1. Your organization conducting critical business processes via email
2. Your organization sending critical business information without verifying recipients

Let’s start with number one. It is easy to imagine why receiving a request from a CEO for a wire transfer via email does not set off the alarm if it is normal for your company to run operations through your inbox. Stop using email for anything of value, or any information that is sensitive, confidential or that authorizes the funds to go from point A to B.

Don’t send routing information over email. Don’t discuss contract details over email. Email is and will forever be subject to “human error and technology failures,” as former CEO of Equifax put it. Not applying the patch and reliance on scanners will not help us win this game. Email is no longer a responsible tool for sensitive communications.

The failure to verify the person on the other end of your conversation is another key component of most BEC campaigns. It is not easy to vet everyone you talk to, and social engineering certainly isn’t making this easier. Ultimately, speed, stress, and inconvenience lead us to make the mistake of conducting business with unverified parties. But still, verification should not be optional when you are transferring money or sharing high-target pricing strategies or negotiating a deal. It is negligent to not take advantage of user verification capabilities supported by math and encryption to ensure that your intended recipient is, in fact, the recipient you think it is.
Moving your critical operations away from email and to a controlled secure workspace where user key verification is built-in is a strong step in boosting your organization’s resilience to BEC. Developing a clear and easily enforceable policy is next:

- Have a policy to NOT conduct business or send sensitive information over email.
- Anyone who asks to conduct business or send sensitive information over email should be subject to extra verification.
- Never respond to an email to wire money.
- Always get a voice or video verification before wiring any funds.
- If you get a suspicious email, save it — do not respond or click any links.
- Ensure that your organization’s procedures mandate that information is never sent via email to reduce the risks from BEC attacks.

For example, with Wickr Pro, you can choose to require video key verification to ensure you are communicating with the right person. Enabled by encryption, you can easily establish a verifiable secure communication channel. You only need to get verification right once to ensure you have the right person on the other end of your business conversation.

Making a change in your organization’s internal policy to never conduct important business via email in and of itself becomes a verification enabler. If your company makes it clear that critical communications and sensitive transactions DO NOT TAKE PLACE in email, the person asking you to transact through your inbox is automatically qualified as not legitimate. A sophisticated attacker might send a joke about the drinks you shared poolside at the company picnic (information grabbed on Facebook) or say something about a good lunch meeting you had with a client (Chatter) or that you closed out tickets from the last sprint (compromised Slack). But if they attempt to initiate a money transfer in an email or discuss proprietary business matters, you and your team instantly know it is not legit.

It is time to move sensitive communications out of easily compromised and discoverable channels. Neither email nor IM is safe. Using these channels today is the same as knowingly clicking on a link from the Nigerian Prince. It is simply negligent.

With tools like Wickr, you can send sensitive information like account routing information and ensure that, after legitimate transfers and communications are complete, all valuable information is deleted according to your organization’s information governance (defensible deletion) policies. You can proactively set an expiration date for sensitive communications to comply with internal and external industry requirements and then rely upon math rather than end users or service providers to protect your data.

Being aware of BEC and having protocols in place to protect against it is vital to protect your business from cyber attacks. It is this reason that secure messaging platforms like Wickr are becoming the smart way to conduct important business.
A Deeper Look Into Managed Secure Messaging

Secure Messaging (SM) platforms are an increasingly vital tool for both individuals and entire organizations to protect themselves from a wide variety of threats. However, there is a distinction to be made between Managed SM (MSM) platforms and (the much more common) Unmanaged ones (USM).

— Unmanaged vs. Managed

Unmanaged SM

Put simply, an unmanaged SM is a single global network managed centrally by a single service provider; e.g. Wickr Messenger. Intuitively, in a USM there are only two types of non-adversarial actors; users (which make up the end-points in the communication network) and the service provider, whose most important job is to maintain the infrastructure (and, usually, the code base/protocol) upon which the distributed system relies.

Managed SM

In a Managed SM platform, there is a third type of actor — namely, the administrator. Rather than being a single global network like a USM, an MSM is really a collection of distinct sub-networks. Each subnet belongs to, and is managed by, its own admin, while each user belongs to a particular home subnet. In other words, Alice@Net1 is a different user than Alice@Net2. In a federated MSM, users on different subnets can, in general, still communicate with each other across subnet boundaries.

— Why Managed Messaging Makes Sense for Almost Any Organization

The more people communicate within the context of some centralized, hierarchical, and/or closed group, the more appropriate an MSM becomes. Here are just a few examples of how natural power and relationship structures in an organization are reflected in an MSM.

Membership

In almost all organizations (be they government, business, NGOs, etc.), membership of a given individual is not (exclusively) up to that individual. Rather, it is decided upon by the organization itself.

How should this be reflected in the organization's communication system? Suppose, for example, a company ends its employment of an employee. Then it is very much in the interest of the company to have the capability to immediately and unilaterally (i.e. at their own discretion) remove the former employee from any and all company internal communications channels. This need is directly reflected by the capability of an MSM admin to de-provision user accounts.
Controlled Information Flows

Another example of structures arising naturally in most organizations (that should be reflected in the secure messaging platform) is information boundaries. Typically, membership in an organization confers new information access and communication privileges upon the member compared to non-members. For example, employees could be privy to secret business intel which they need to discuss with each other that should not leak to non-employees.

An MSM can be a useful tool for reflecting and enforcing such natural boundaries via network segmentation. For example, users that have no legitimate need to communicate with external individuals can simply have that capability removed by the admin. In fact, beyond protecting against adversaries, the biggest concrete benefit of network segmentation of communications is the reduction of the risk of unintentional information leakage. For example, with appropriate segmentation in place, there is no more risk of mistakenly CC’ing outside parties on sensitive communications.

More generally, having a trained admin set security policy rather than leaving such choices up to each user helps avoid unintentional security lapses due to poor configuration by untrained users. It is as unreasonable to expect every last member of your organization to have sufficient security knowledge to make policy decisions correctly as it is to hope that a one-size-fits-all security policy decided upon by a global service provider of a USM will be the right choice for your particular organization.

Private Infrastructure

Finally, for organizations with extremely sensitive comms, it can be worthwhile to invest in a communication system that allows explicitly routing all internal communications exclusively via an organization-owned and controlled infrastructure. For example, this can be particularly useful in defending against government surveillance and traffic analysis, as well as to limit exposure to upstream ISPs and the SM platform’s service provider. Here too, MSMs (at least those with on-premise capabilities) will be of particular interest to achieve these security goals.
Managing Data Governance in Your Enterprise

The benefits and pitfalls of deploying enterprise-grade solutions are the policies around data governance and the proper use of collaboration platforms. Once organizations have a fully vetted policy in place, the design aspects around proper use are more easily implemented.

A couple of important topics come into play when we work with our customers: Scale & Authorization. When we talk about Scale, it involves both capacity and building cross-collaborative networks. When we address Authorization, the questions and discussions lead to:

“How do I provide a secure environment for our executives to discuss Board-level topics, such as:"
• M&A
• Fundraising
• Corporate Structures

“How do I restrict information that’s only intended for internal audiences, like:"
• Human Resources
• Research & Development
• Crisis Management

“I’d like to group users into certain information control profiles”
• Business Unit categorization

“I have trusted 3rd parties I need to communicate with, how do we accomplish this?”
• Outside Corporate Counsel
• Incident Response
• Vendor Management

In order to address these topics, you must have a secure collaboration solution in place that allows strict policy enforcement — the ability to create tightly enforced Access Control Lists between users and networks.

While establishing a system architecture and placing users in the proper security groups, some organizations may want to integrate additional controls like Data Loss Protection, Active Directory/LDAP or communications archiving for eDiscovery/Risk/Auditing — all of these capabilities should be part of your overall plan when designing and deploying your end-to-end encrypted collaboration solution.

In the end, Zero Trust is not a blunt object - it should be flexible enough to create specific processes for established policies and needs across your organization.
Wickr Enterprise

Unrivaled Data Protection, Business Collaboration, and Regulatory Compliance

Wickr Enterprise combines the privacy, security, and data minimization of our free consumer and business SaaS apps with a compliance service that gives regulated organizations the ability to retain communications when necessary. Wickr Enterprise is deployed on-premise, or in a dedicated cloud environment to give total control to the customer. With Wickr Enterprise, companies proactively enforce information governance policies to ensure that no conversation lives beyond its useful life on end points. The majority of communications don’t need to live forever on providers’ servers for them to monetize or on end user devices for attackers to breach. Wickr is simply a smarter way to do business and manage risk in regulated environments.

Teams doing critical work in business, security, government, R&D, and other areas now choose to use math to protect data rather than rely on overstressed technical teams or trust the good intentions of service providers. Millions of Wickr customers encrypt communications and data proactively, set expiration time to maintain good security hygiene, and verify participants in high-target conversations.

Wickr Enterprise was built to enable both compliance and data protection so that our most important institutions can deploy next-generation defense capabilities to defend against their most advanced adversaries. Sensitive communication systems across our democratic institutions, critical enterprises, and infrastructure require the strongest protection possible. Wickr Enterprise and its Compliance Service are engineered to meet any record retention, auditing, and data security requirements for regulated industries. It is specifically designed to enable organizations to enforce transparency and accountability in compliance with statutory data retention standards (i.e. FINRA, PRA, FRA, FOIA) while ensuring maximum security of high-target communications.

“Data at rest equals data at risk. If your corporate data lives on too many devices or someone else’s cloud, your enterprise is at risk. If your critical business information and transactions are in email, your organization is at risk. Whether you are a government or a financial institution, Wickr Enterprise means both – immutable audit and data protection, so you are not at risk and in compliance.”

— Gilman Louie, Alsop Louie Partners

Wickr Enterprise is by design deployed and operated by the customer’s own security and IT teams, and on their own infrastructure. Wickr remains outside of the self-hosted enterprise networks and never holds access to keys or content for stronger data security. All communications are encrypted and ephemeral on the end user devices to protect against compromise or theft, while allowing for integrations with industry’s leading archiving systems to maintain safe, auditable, and immutable record keeping.

Learn more about Wickr Enterprise