CYBERSECURITY &
BUSINESS GROWTH:

Turn Your Program into a Profit Center

GreyCastle
security

WHAT'S INSIDE

UNDERSTANDING THE VALUE OF CYBERSECURITY

When most companies think about cybersecurity, they're considering things like regulatory compliance, loss prevention, and qualitative risk reduction – all valuable facets of a well-rounded program. But with the right strategies and implementation, a well-managed cybersecurity program has a major impact on driving revenue, reputation, and company growth.

Companies of all sizes are exploring digital technologies more than ever to build better-connected audiences, increase operational agility, and create web-based ecosystems that offer new revenue streams. With such a prevalence of digital services and solutions, opportunities to extract more value from your cybersecurity program are ever-growing.

The global average cost of a data breach in 2020: $3.68 million.[1]

CYBERSECURITY & CUSTOMER LOYALTY

It often feels like we can't go a day without hearing about another data breach at a major corporation or social network, from sensitive data to private customer information to intellectual properties. These stories generate urgency around better cybersecurity and provide opportunities for you to demonstrate how you protect your own customers, increasing the likelihood of retaining and gaining privacy-conscious customers who want reassurance. The most successful tech giants make it abundantly clear how they incorporate various layers of security and encryption in their hardware, software, data storage products and services and leverage their mindset and methodologies as benefits of being a customer within their ecosystem.

Whether you handle customer contact information, personal histories, financial data, health records, or other sensitive data, the way you protect that information and communicate your practices, beyond obeying regulatory demands, has a substantial impact on building customer trust and ensuring continued loyalty.

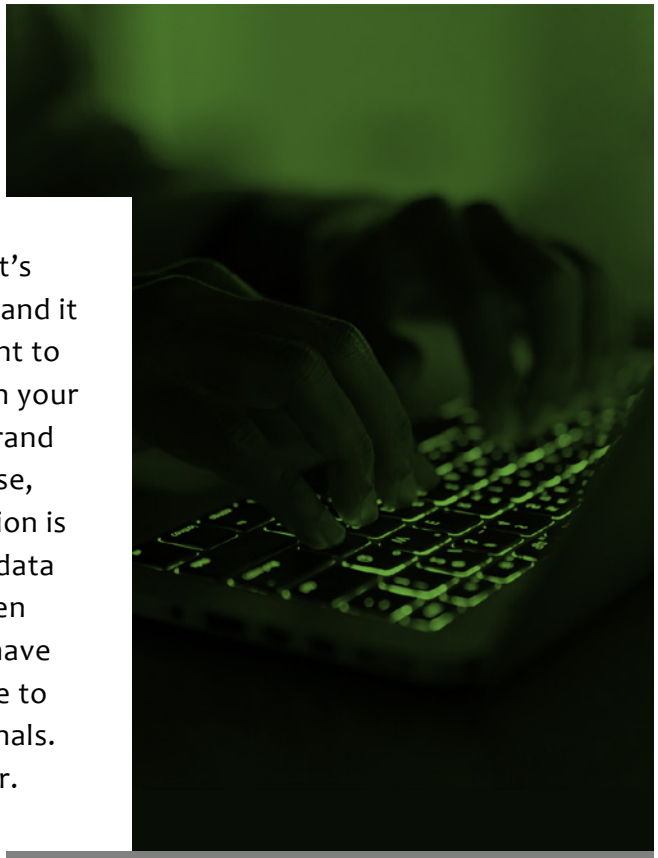
79%

of Americans report being concerned about how companies use and handle their data.[2]

CYBERSECURITY & BRAND REPUTATION

From small local establishments to global conglomerates, brands of all sizes can be catastrophically impacted by the unwanted media attention and exposure that often come with a hack or data breach.

Your brand is your company's identity; it's the most visible asset of your business, and it must be protected to ensure others want to continue doing business with you. When your company suffers an attack or breach, brand trust can be severely damaged. Of course, the key to upholding a spotless reputation is to remain vigilant and avoid things like data breaches altogether. Unfortunately, even the most well-defended organizations have weaknesses, and no company is immune to the ingenuity of determined cybercriminals. But that doesn't mean you can't recover.

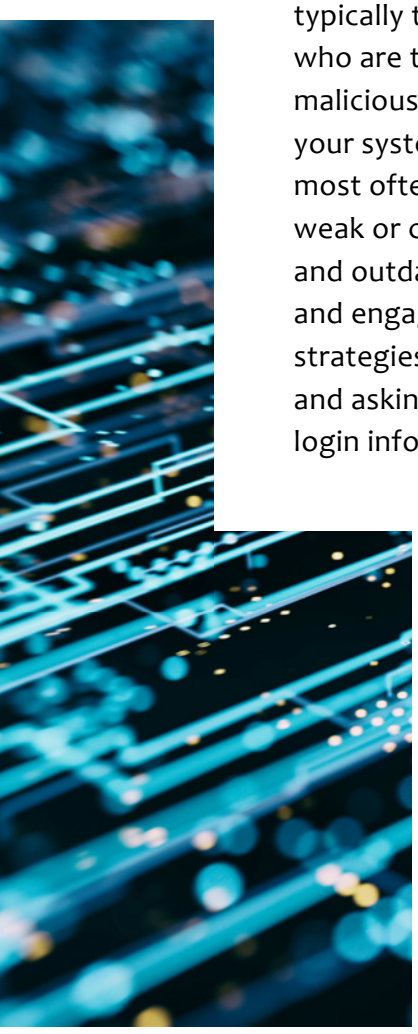


Your immediate response and remediation in the wake of an attack also play a massive role in how you're seen by the public. The speed with which you resecure your systems, find out what went wrong, and implement changes that leave you better prepared for the future go a long way in maintaining a positive or salvageable reputation.

The most common attack vectors in 2020 include compromised credentials, cloud misconfiguration, and third-party vulnerabilities.[1]

CYBERSECURITY & FINANCIAL STABILITY

Estimates from The Ponemon Institute show that the global average cost of a data breach in 2020 was $3.68 million. That number varies by industry, but no matter what, it's pretty daunting! It's also a common misconception that these types of losses are typically the result of elite hackers who are tirelessly working on malicious code to compromise your systems. In reality, they're most often taking advantage of weak or compromised passwords and outdated security methods and engaging in social engineering strategies, such as calling a helpdesk and asking for a password reset or login information.



Whether cybercriminals spend weeks trying to gain entry into your systems or have the door opened for them in mere minutes, the results can be catastrophic. A well-planned, monitored, and maintained cybersecurity program helps you avoid these massive financial blows and gives you greater agility to respond and mitigate any damage if and when an incident does occur.

Average cost of a breach among organizations with fully deployed cybersecurity security automation:

$2.45 million[1]

Average cost of a breach among organizations without cybersecurity automation:

$6.03 million[1]

MAXIMIZE THE VALUE OF YOUR CYBERSECURITY PROGRAM

As the potential costs of a data breach only continue to grow, it's up to you to put safeguards in place that secure your data and follow all legal guidelines and put your customers at ease and position your business as a trusted name in your industry. GreyCastle Security is here to help you. Contact us today to consult about your current cybersecurity program and get the support you need to maximize the value you get from your investment.

1. Cost of a Data Breach Report 2020, The Ponemon Institute, https://www.ibm.com/security/digital-assets/cost-data-breach-report/
2. Americans and Privacy, Pew Research Center, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

For more information about protecting your organization from cyber threats, contact GreyCastle Security.

Email us at intel@greycastlesecurity.com or give us a call: (518) 274-7233

www.GreyCastleSecurity.com | @greycastlesec