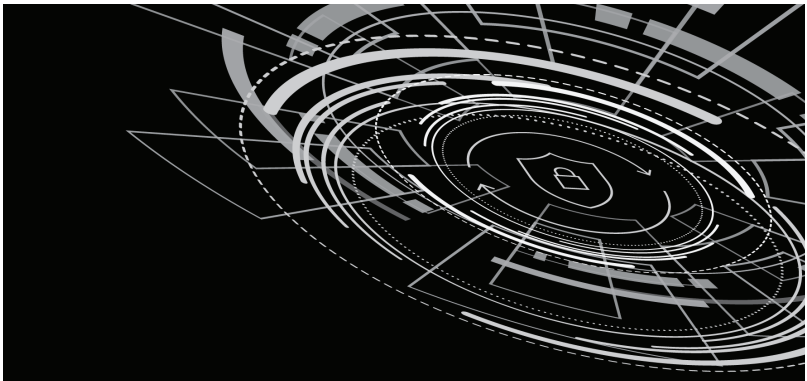
CYBERSECURITY:
THE SILENT BATTLEFIELD

Leverage The Power Of Cybersecurity
With Compliance To Defend Your Business
From Invisible Cyber Predators

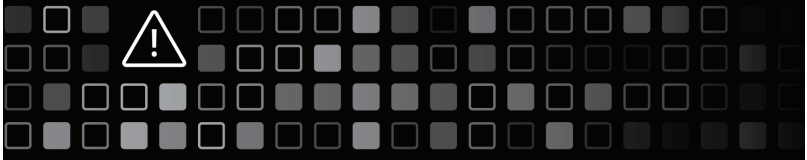
CHRIS GOTSTEIN

FEATURING CYBERSECURITY
EXPERTS FROM AROUND THE WORLD



CYBERSECURITY:
THE SILENT BATTLEFIELD

Leverage The Power Of Cybersecurity With Compliance To Defend Your Business From Invisible Cyber Predators



FEATURING CYBERSECURITY EXPERTS FROM AROUND THE WORLD

BigRedMedia
a TMT company

Nashville, Tennessee

Chapter 7:
Honesty In Cybersecurity: A Nonnegotiable Business Practice

Chris Gotstein
Founder and President, GoTech IT Solutions

A 2006 Ipsos survey found that 64% of Americans believe lying is sometimes justified. While that might seem high, the lies they are referring to include "white lies," such as saying you're having a good day when you're not, telling someone you like their shirt when you don't, or telling a friend the cake they baked was delicious when it really tasted like pavement. Tiny, harmless lies that we all rely on in everyday life to avoid explaining ourselves or hurting people's feelings. However, cybersecurity is one area where it is not okay to tell any type of lie, as the consequences can be devastating for your business, clients, and vendors. In this chapter, I want to highlight three cybersecurity-related instances where, as Benjamin Franklin famously wrote, "honesty is the best policy."

The first involves a recent conversation I had with a subcontractor who supplies Department of Defense contractors. We reviewed their network infrastructure and cybersecurity services to see if they met DoD contract requirements. To be eligible to fulfill a DoD-related contract, subcontractors must meet specific requirements, such as the Defense

Federal Acquisition Regulation Supplement (DFARS), International Traffic in Arms Regulations (ITAR), and, most recently, Cybersecurity Maturity Model Certification (CMMC), and then verify what they've done by checking a row of boxes on a form. My contact told me that, for years, they've just been checking the boxes and sending the form in.

They do this for three primary reasons. The first reason is that they feel their business is too small to be the target of an attack – a common justification. The second reason is that they don't understand what's required of them and assume that their current IT provider is taking care of it. The third reason is that they feel it will be too expensive to become CMMC compliant (CMMC is the certification required for DoD contractors and subcontractors). After all, why spend money and time when you can just check a row of boxes in under 30 seconds?

Their actions have had no immediate ramifications because filling out the form attesting to the DoD's stringent cybersecurity requirements is based on the honor system. The honor system is cost-effective for the government and convenient for businesses. And while some studies show it encourages trust and integrity, it makes it extremely easy for companies to abuse the system if they're so inclined.

Dishonesty Can Cost You

While I appreciate the DoD subcontractor's honesty with me and empathize with his business's situation, they would be better served if they were honest with themselves, their clients, and the government. If a hack occurs, they will most likely face fines and penalties in addition to losing productivity because of downtime. Plus, they could lose their access to all DoD-related contracts. If they have cyber insurance, once the insurance company finds out they lied about their cybersecurity

situation, they will deny their claim. Their business's reputation will be tarnished forever, and financial losses could force them to shut down permanently.

A Pathway To More Significant Damage

However, their lack of honesty could have far more significant consequences. Here's the thing: 82% of ransomware attacks in 2021 were against companies with fewer than 1,000 employees, and 37% involved companies with fewer than 100 employees. Hackers target smaller businesses because small businesses tend to have weaker cybersecurity measures than large companies. This makes them easy prey for cybercriminals. Hackers know that smaller companies often have access to a larger company's network or data. A hacker will target a smaller company using phishing, malware, social engineering, etc., and gain a foothold within their network. They then look for credentials, access to email, sensitive files, or direct connections (such as a VPN, AWS, or Azure) to a larger company's network. If they don't find anything, they move laterally to another business until they find a way to infiltrate the larger company's systems.

U.S. Generals Put At Risk

As a result, the DoD subcontractor is not just putting their business at risk; they are also putting every company they deal with at risk. In 2019, a security breach involved AutoClerk, the reservations management system owned by Best Western Hotels & Resorts group. Over 100,000 records were exposed, including those of the U.S. government and military personnel. Personal information included travel plan details of U.S. generals – information that could have resulted in physical harm to the affected personnel. The AutoClerk breach highlights the

vulnerabilities of third-party contractors handling sensitive information and the risks arising when compliance obligations are ignored.

A National Security Risk

In 2016, Chinese hackers infiltrated the computer systems of a major U.S. defense contractor by gaining access through a subcontractor. They then stole F-35 fighter jet plans. The subcontractor, an unnamed Australian company, was small, with only a one-person IT department, contributing to its vulnerability to being the target of a cyberattack. This breach advanced China's military capabilities and exacerbated tensions between China and the U.S. So, while my DoD subcontractor prospect might think his dishonesty comes with no ramifications, the reality is that every subcontractor who checks the boxes without doing what is required could very well be putting the United States national security at risk.

No Business Is Too Small To Be Hacked

Let's examine the three reasons my prospect gave to justify his dishonesty. His first reason was that he felt his business was too small to be hacked. I believe I've proven that he's not too small to be hacked, but he probably feels this way because, for the most part, only the large cybersecurity breaches get reported by the media. Studies show that cybercriminals are three times more likely to target small businesses than larger companies. His second reason was that he didn't understand what was required of them. This, of course, is not a justification. (A form of this excuse is that they assume they have cybersecurity measures in place and give themselves the benefit of the doubt.) Cybersecurity compliance is a contractual obligation for the vast majority of companies that handle client data. Businesses are expected to be proactive vs.

reactive. This goes for any small business with compliance requirements, from health care providers like dentists and small medical practices to financial advisors and accountants needing to protect their clients' data and privacy to meet FTC Safeguard regulations.

Understanding The Value Of Cybersecurity

His third reason was that he felt cybersecurity was too expensive. Except for nonprofit organizations, almost every business is in business to make a profit. I get it, but it comes down to your understanding of technology and the value you put on it. If you don't value technology, it will be a low-priority item in your budget. A typical small business should spend at least 6.9% of its budget on technology. The subcontractor in question had a contract valued at $5 million to supply DoD parts. With a contract for $5 million, if it was the only business they did all year, their IT budget should be $345,000 (6.9% of $5,000,000 = $345,000). My proposal to fully secure their business with managed IT services at that time was $2,500 a month ($30,000 a year).

In many cases, it's been my experience that it's not that a business can't afford to spend the money. It's because they *don't want* to spend the money and do not see the value in technology or cybersecurity protections. Business owners and managers need to understand the value of cybersecurity and compliance and make it a priority for their business. If they don't, they could wake up one day and find their business has been hacked, and, in mere seconds, their business's reputation and survival could be in serious jeopardy – with their cybersecurity insurance provider refusing to cover any of the costs.

Keeping Everyone Honest

The second "honesty area" concerns your IT provider. It's more about ensuring transparency and accountability than suggesting that your IT provider is intentionally dishonest. To promote our services, we will occasionally offer a prospect a free internal penetration test (also called an internal cybersecurity audit) to determine if what your IT provider has promised is what they are delivering. Our findings are often eye-opening. About half of the prospects fail the test, and we find gaping holes in their cybersecurity. We then review with them what their provider is doing, what they're not doing, and what they said they were doing but are not doing.

Trust, But Verify

When we find discrepancies, we note that while the IT provider could be dishonest, chances are the reason is more benign. IT services are complex and multifaceted. Ensuring everything is correctly implemented requires meticulous attention to detail – details that are sometimes overlooked. Plus, there could have been miscommunication between the IT provider and their client, assumptions made, or a lack of thorough verification. And, of course, human error might also have been a factor. It's important to note that we don't do the assessment ourselves when we offer a potential client a free cybersecurity assessment. To avoid any bias, we use a third-party company. We also do quarterly assessments on ourselves as a company and as a compliance add-on to existing clients to ensure we deliver what we've promised.

Ignorance Is No Excuse

If you are legally obligated to be CMMC compliant or meet any other compliance or industry standard, and a breach happens, and it's

determined that the cause was something your IT provider should have been doing but wasn't, the fact that your IT provider wasn't doing their job is not a valid excuse. It's *your* responsibility to make sure your business is compliant. This includes third-party or internal testing to ensure all presumed services are in place. However, IT companies have a moral and legal responsibility to make good on their obligations. If they have not implemented everything they should have, it's not uncommon for insurance companies to sue the IT company for damages.

Don't Assume

To ensure your business receives all the services promised by your IT provider, you need to have clear and continuous communication – regular updates, progress reports, feedback loops – with them. You need a robust service-level agreement and statement of work that details the design, development, deployment, and management of IT services. Plus, you need continuous monitoring to track the effectiveness of your IT services, and you need to do regular audits and assessments. An honest IT provider will show you exactly what they are doing and encourage you to bring in a third-party company to provide you with verification. Honesty means you can verify that cybersecurity protections, policies, and procedures are in place rather than just assuming they are.

Honesty And Transparency Equal Trust

The other key area where you need to be honest is with your public and client relations after a cyberattack. No business wants to admit they were hacked. When you're still reeling from the shock, anger, and embarrassment of being the victim of a cyberattack, the tendency might be to try to do whatever you can to keep the news from getting out. Honesty and transparency are crucial for maintaining trust with your

clients and the public. Email, phone, or mail your customers directly and as quickly as possible. Notify the public through the press or trade magazines. A press release is an effective way to reach your customers, stakeholders, and the media.

Turn A Negative Into A Positive

Your message should contain the details of the breach, what information was compromised, the steps you are taking to resolve the issue, and what experts are assisting you. You should also apologize to your customers for the inconvenience caused and accept full responsibility. It's essential to use clear and straightforward language. Avoid complex explanations and technical jargon, which could confuse people. You must keep your customers and the public informed on an ongoing basis. Let your customers know what they should be doing to protect themselves. For example, if their credit card information was compromised, advise them to contact the issuer and request a new card with a different number. Consider offering your customers credit monitoring or an identity protection service. If you handle yourself with grace during the aftermath of a cyberattack, you can bolster your reputation as a trustworthy and honest business.

Honesty Is Nonnegotiable

While I've touched on only three instances where honesty is imperative, honesty is essential in every aspect of cybersecurity. To create a culture of honesty and integrity in your business, start from the top, with the owners and management fully invested. If upper management doesn't prioritize cybersecurity transparency, your employees won't either. Encourage your employees to report cybersecurity incidents without fear of repercussions. Doing so fosters a culture of openness.

Encourage honesty about mistakes. Ask your employees for honest feedback about your training programs. This will lead to continuous improvement. Be a business that is honest and trustworthy every step of the way – from checking a box on a compliance form to training your employees on how to substantially reduce the odds that your business will be the victim of a cyberattack. When it comes to cybersecurity, honesty truly is the one nonnegotiable business practice.

About Chris Gotstein

Chris Gotstein is the founder and president of GoTech IT Solutions. Although he founded GoTech in 2013, Chris has been in IT for over 25 years. With offices in metro Milwaukee and Michigan's Upper Peninsula, GoTech provides IT and cybersecurity services to small and midsize companies throughout Eastern Wisconsin and the Upper Peninsula of Michigan.

Chris's interest in technology started in the late '80s when he accessed computers through his parents' business. Inspired by them, he aspired to own a business. He enhanced his tech skills in high school by setting up computer networks and offering tech support. Chris earned a bachelor of business administration from the University of Wisconsin-Whitewater, minoring in computer support and networking.

He began his professional journey in technology as IT support for the College of Business and Economics at UW-Whitewater. Prior to graduating, he secured the role of technology support specialist for a Milwaukee-area school district, a position he held for five years. As the sole IT person for the entire district, Chris handled day-to-day support and long-term technology planning, significantly strengthening his expertise and problem-solving skills.

Chris moved to Norway, Michigan, to work for a small Internet provider focusing on enhancing rural connectivity. This role diversified his tech skills and understanding. He also began consulting for small businesses, leading to the founding of GoTech IT Solutions. Chris holds several industry certifications (including Cybersecurity Maturity

Model Certification Registered Practitioner credentials), establishing GoTech as a leader in cybersecurity for small businesses.

GoTech IT Solutions sets itself apart by emphasizing building strong client relationships. Chris believes being seen as a partner rather than just a vendor is crucial. To achieve this partnership, GoTech holds regular technology business reviews with all clients to discuss emerging technologies, cybersecurity compliance, and new efficiencies to help clients' growth goals. This philosophy extends to the company culture, where the team is dedicated to resolving issues, maintaining efficiency, and helping clients grow with technology through continuous education.

Chris is firmly committed to community service and technology enhancement for nonprofits. His journey began with volunteering on municipal committees, which led to his election to the city council in the City of Norway. He has served on various boards, including the local Chamber of Commerce, and ensures that his company, GoTech, donates to nonprofits, such as the Wounded Warrior Project. In addition to fulfilling these roles, Chris dedicates his efforts to helping nonprofits improve their technology use and cybersecurity, providing support that aligns with their budgets, and donating time and materials as needed.

Chris and his wife, Rachael, love to travel. They have especially enjoyed road trips throughout the U.S. with their daughter, Chloe. Chris enjoys remodeling and landscaping projects around his home in his spare time and helping others do the same. He also enjoys playing sports, photography, and hiking adventures with his wife.

For more information, contact Chris Gotstein at GoTech IT Solutions:
Phone: 262-649-2343
LinkedIn: linkedin.com/in/chrisgotstein
Email: chris@gotechits.com
Web: gotechitsolutions.com

CYBERSECURITY:
THE SILENT BATTLEFIELD

ABOUT CHRIS GOTSTEIN

With over 25 years in the IT industry, Chris Gotstein is the founder and president of GoTech IT Solutions, a leading provider of IT and cybersecurity services for small and midsize businesses across Eastern Wisconsin and Michigan's Upper Peninsula. Since founding GoTech in 2013, Chris has been dedicated to helping businesses leverage technology securely and efficiently.

Chris's passion for technology began in the late 1980s when he first accessed computers through his parents' business. Inspired by their entrepreneurial spirit, he envisioned running his own company one day. In high school, he honed his skills by setting up computer networks and providing tech support, a foundation that propelled him toward a career in IT. He later earned a Bachelor of Business Administration from the University of Wisconsin-Whitewater, minoring in computer support and networking.

Chris started his professional journey as IT support for UW-Whitewater's College of Business and Economics before securing a position as a technology support specialist for a Milwaukee-area school district. As the district's sole IT professional, he managed daily support and long-term technology planning, sharpening his problem-solving skills. Later, he expanded his expertise by working for a small internet provider in Norway, Michigan, where he focused on improving rural connectivity. During this time, he also began consulting for small businesses, which ultimately led him to establish GoTech IT Solutions.

A certified Cybersecurity Maturity Model Certification (CMMC) Registered Practitioner, Chris has positioned GoTech as a trusted leader in cybersecurity for small businesses. He prioritizes building long-term client partnerships rather than acting as a traditional IT vendor. Through regular technology business reviews, GoTech helps clients stay ahead of emerging technologies, strengthen cybersecurity compliance, and optimize IT strategies to support their growth.

Beyond his business, Chris is deeply committed to community service. He has served on municipal committees, held a city council seat in Norway, Michigan, and actively participates in various boards, including the local Chamber of Commerce. His company, GoTech, donates to nonprofits such as the Wounded Warrior Project, and he frequently helps nonprofits enhance their cybersecurity and technology infrastructure by offering support, resources, and donations.

Outside of work, Chris enjoys traveling with his wife, Rachael, and their daughter, Chloe—especially on road trips across the U.S. He also spends his free time on home remodeling and landscaping projects, playing sports, photography, and hiking adventures with his wife.

Designed and Produced by Big Red Media
Printed in the USA

BigRedMedia
a TMT company