



Dale Stein
Co-Founder

Attackers Have Successfully Hit the Nation’s Largest Corporations – Their Onslaught on SMBs Will be Worse – Are You Prepared?

Leading Managed Technology Services Provider Shares How SMBs Can Protect Themselves from Cyberattacks and Ransomware Threats

LOS ANGELES/VENTURA/ORANGE COUNTY/SAN DIEGO – July 29, 2021 – i-NETT, a leading managed technology services provider (MTSP), recently shared that some of the nation’s largest corporations, like McDonalds, Adobe, eBay, Equifax, LinkedIn, Marriott, Target and Yahoo have all been affected by cybersecurity breaches. While many of these breaches have been widely publicized, they only represent a small fraction of the attempted cyberattacks, which the modern business owner now faces. As a result of these breaches, we are also beginning to see cybercriminals become more emboldened, targeting more critical infrastructure in an effort to demand heftier sums. In fact, recently the Colonial Pipeline, which is responsible for supplying 45% of the fuel for the East Coast, was hit with a ransomware attack. This halted gas distribution, sending customers into “panic buying” throughout the East Coast and eventually cost \$4.4 million to restore.

Meanwhile, JBS, one of the nation’s largest meat processors who is responsible for 20% of the nation’s meat supply, was also hit with a ransomware attack that they eventually paid \$11 million to resolve. While most SMBs are aware of the growing threats posed by cybercriminals, they are failing to recognize that after large corporations and major infrastructure centers fortify their cyber defenses, hackers will have no place to turn but to small business.

i-NETT has been doing its best to educate business owners on the challenges that a breach, virus or phishing attack could have on any organization, and its best summarized by this statistic from the National Cyber Security Alliance, “60 percent of small and mid-sized businesses that are hacked go out of business within six months.” While daunting, all this statistic actually reveals is that any preventative actions taken now, could have dramatic impacts on helping an SMB avoid these kinds of disruptions. “It’s always a delicate balance,” states Dale Stein, Co-Founder of i-NETT. “We consider it our duty to be honest in regards to the scale and scope of cyberattacks in the modern era, however, there’s so much that businesses can do to

protect themselves, so that they don’t have to worry about these sorts of nuisances affecting them.”

While an anti-virus and firewall may have been an effective security measure in the early 1990s, technology has evolved dramatically since then. There are many other technology systems available, that can fortify any SMB’s defenses so that they are fully prepared and protected. Here are 6 steps that any SMB can take to protect its staff, customers and future from cybersecurity disturbances.

1. Use “Layers of Security”
- Taking a layered approach to security enables damage to be quarantined, while simultaneously reducing the severity of any attack. This can easily be set up as long as the network administrator has taken good care to keep the infrastructure well-organized and properly maintained.

2. Activate Multi-Factor or “2-Step” Authentication - Most companies now require multi-factor authentication upon logging into key systems, requiring the user to confirm their identity before proceeding further, via text message or phone call. While this is likely to become ubiquitous across all platforms, especially cloud apps, other

internal technology systems need to be configured to provide this basic, yet extremely effective layer of security.

3. Have a Data Backup or Data Recovery Plan - In the event of a breach or an outage, it's extremely useful to have all key data duplicated and stored securely in a remote location. Not only does this thwart less sophisticated cybercriminals who are counting on their target to be underprepared, but it eliminates the downtime that any breach or outage could cause, while employees "get things back up to speed."

4. Use a SOC (Security Operations Center) - In the same way that residential homes are supported by a remote security center, with 24/7 monitoring, notification and authority alerting capabilities, your team's devices should be similarly supported, as well. A good SOC will monitor network traffic, endpoints, logs, security events, etc., so that analysts can use this information to identify vulnerabilities and prevent breaches. When a suspicious activity is detected, your platform should create an alert, indicating further investigation is required.

5. Mandatory Cybersecurity Trainings for Employees - Unfortunately, "human error" is one of the main causes of most security breaches. If a company

has not mandated cybersecurity trainings for employees, then undereducated employees can accidentally serve as a hacker's greatest ally. These employee trainings do not take very much time to complete and they can be configured to track and confirm employee progress.

6. Remove All IT Tasks from the CEO's List of Responsibilities - Not only is the CEO typically one of the people with the least amount of technical know-how in the company, but the time consumption required to build an adequate cyber defense strategy is sizable. While CEOs typically feel an obligation to keep their team protected, CEOs should be spending the majority of their time thinking strategically and focusing on how to create more opportunities for revenue growth, not tinkering with IT tools that they don't have full mastery over. At this stage, consider consulting with or hiring an expert IT advisor to guide you through the nitty-gritty of installations, monitoring and ongoing management of critical security systems.

While hackers continue to search for targets, the steps outlined above are immediately actionable and will serve as a solid foundation for the majority of businesses that wish to prepare themselves for the coming trend.

ABOUT I-NETT

Founded in 1982, i-NETT is Southern California's leading data and voice company. The company's mission is to increase its customers' profitability, improve their productivity and give them a competitive advantage by implementing the right technology. i-NETT is the only provider that protects its customers from the two risks of technology - obsolescence and cost. As its customers' trusted technology advisor, i-NETT has earned the position as the market leader and its customers' business through quality products and services.

i-NETT is a premier Member of Technology Assurance Group, an organization of leading managed technology services providers (MTSPs) in the United States and Canada representing \$500 million in products and services. This means that the organization is the ultimate resource for business phone systems (VoIP and Session Initiation Protocol (SIP) provisioning), Managed IT Services, Cybersecurity, Video Conferencing and Disaster Recovery.

i-NETT delivers future technology today! For more information, please visit please call 805.642.3558 or visit us at www.i-nett.com.