Cyber Lantern: Integrating Security in Uncertain Times

The Remote Work Paradox

Today, organizations and businesses of all sizes have been mandated to shift employee operations away from onsite work to a remote work-from-home reality. This presents a logistical and security compliance challenge for Small and Medium-Sized Businesses (SMBs) who: 1) cannot afford to provide all of their workforce with a laptop and/or a secure IT infrastructure, and 2) who have not put into place a distributed security operations team who can remotely respond to and mitigate online threats. While this is not as big of a cost concern for larger businesses like Facebook, Google, and Amazon, the options are seemingly limited for SMBs of 500 employees or less and government institutions who were already struggling to keep up with securing and monitoring their networks and operations. After the initial scramble to get employees working from home productively, many businesses were beset by another problem: remote workers are not as secure as those working on-premises.

Cybercrime reports have quadrupled since the start of the year, due in large part to the number of employees now working from home. Small businesses or local governments do not have the luxury of a dedicated security team to help them fight the attacks that their staff are encountering. “Human hacking” is on the rise – in the office, you could walk down the hall to ask Brenda if she really sent out a link to an invoice with no context. At home, employees are much more likely to simply click on risky links rather than email or call a teammate to confirm its origins. To make matters worse, this time of uncertainty has led to a higher likelihood for an employee to click on unknown links under the impression they are coming from legitimate sources providing information on the pandemic as it relates to work, and daily life. Remote work has kept employees safe from the pandemic but has led to enormous cybersecurity risks.

Increasing Security with No Budget

While straining under pandemic conditions with fewer clients, many businesses have been forced to furlough or lay off staff to stay afloat. At the precise moment that a business needs to add to their IT team with at least one (or more) security-focused members, the money is not there to pay for it. The associated costs are not just related to salary, as any business owner knows – there are benefits, taxes, and of course, the time to train and get a new employee up to speed. This does not include the cost to continuously train and keep your security workforce prepared for the constantly evolving threats and challenges of cyber.

For a small business, the consideration for adding a security team often was a priority before the pandemic. With an on-site centralized workforce, their small IT team could secure the network easily. With a widely distributed workforce, this is not an option, and presents a very promising target of opportunity. One in seven small businesses have already reported at least one cyberattack since COVID-19 began, and **60% of small businesses close within 6 months** of a data breach. Attackers are also strategically targeting organizations who play critical roles during the pandemic – local governments, hospitals, research facilities and biotech companies. These organizations are crucial now more than ever, making them a perfect target for ransomware attacks requiring victims who were not prepared to pay the ransom to restore business operations. For businesses already struggling with budgets today, a data breach or cyber attack is likely to take them down almost immediately.

Cyber Lantern vs In-House Cost Breakdown

One of the biggest benefits of hiring an external team to help manage your security is that you get the talents and skillset of an entire team for less than the cost of a single employee. Unlike building your own team, Cyber Lantern operates as an “out of the box” solution - with little effort for your team to deploy our services. Our team comes prepared with expert experience in cyber security operations and utilizes our proprietary platform to equip you with state of the art security at affordable costs. Employing an in-house team of your own may seem convenient, but can be resource intensive and lead to high operational costs just to maintain a basic 9 to 5 operation.

Cyber Lantern: Your Solution to Security in Uncertain Times

Security Operations Cost Breakdown

While the cost of running security operations can vary depending on several aspects, SMBs can generally expect to incur annual costs for tool licenses, IT infrastructure and human resources. When you hire the Cyber Lantern team, the cost of human resources is significantly lower, giving you more resources with greater knowledge. Cyber Lantern operates as an extension to your security helping to monitor and detect malicious behaviors in your environment while also providing expert guidance in how to optimize your security while staying within your budget. Additionally, Cyber Lantern operates on its own proprietary SOC platform, allowing your team to cut costs in log management and threat intelligence. This also allows Cyber Lantern to remain product agnostic- meaning all your current security tools do not need to be replaced for us to monitor your environments.

Cost to Not Improve Security

If you fail to engage in any security practices, you're at risk for a data breach, ransomware, or worse; the industry your SMB is in doesn't matter; the cost of cybercrime to the victim is significant. The average breach costs most companies $50k-$500k, accounting for:

- ✓ Cost to remediate
- ✓ Operational downtime
- ✓ Loss of business (old and new)
- ✓ Brand reputation
- ✓ Time to remediate
- ✓ Ransomware payouts
- ✓ Incident Response
- ✓ Brand reputation

Not convinced? Call us today to begin your free 60-day trial.

Average Annual Cost of Security Operations

	SMB Cost (Avg. 250 Employees)	Cyber Lantern Cost
Cost of Tools (Average annual license costs)		
Anti-Virus	$24,000-$60,000	Same as SMB Cost
Log Correlation & SIEM	$24,000-$48,000	INLCUDED
Threat Feed (1-2 feeds)	$6,000-$24,000	INCLUDED
Network Protection	$6,000-$12,000	Same as SMB Cost
Ticket System	$6,000-$14,400	INCLUDED
Cloud Services (for security)	$12,000-$24,000	Same as SMB Cost
Annual Cost of Tools	**$78,000-$182,400**	**$42,000-$96,000 (50% less)**
Cost of Human Resources (Average annual cost for 8 hrs x 5 days a week)		
Mid-level Security Analyst	$120,000	**All inclusive price for 24x7 security operations including:** • **Log Management** • **Monitoring & Detection** • **Data Analytics & Reporting** • **Response & Support**
Senior Security Architect	$150,000	
Security Engineer	$150,000	
Head of Security	$192,000	
Annual Costs of Human Resources	$612,000	
TOTAL ANNUAL COSTS:	**$663,600- 717,600**	**80-90% less than in house***

** Pricing varies by customer size and services rendered. Contact us directly for price quotes.*

In the face of bankruptcy, millions of dollars in fines, lost revenue, auditing, and repairs, the cost of hiring a team of skilled professionals is negligible.

Cyber Lantern, A Digital Lantern Division
Phone: 650-729-8228 E-mail: info@cyberlantern.com

Cyber Lantern