CYBER LANTERN: THE COST OF SECURITY SERVICES

THE REMOTE WORK PARADOX

With a shift to workforce working nearly entirely from home, organizations of all sizes are struggling to adapt. It is one thing for Huge Corporations to send their employees home with a laptop, but what about local government organizations and small to mid-size businesses (SMBs)? After the initial scramble to get employees working from home productively, many businesses were beset by another problem: remote work is not as secure as 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 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. At home, your staff are much more likely to simply click on risky links rather than email or call a teammate to confirm. 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 their staff to try and 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. It is not just 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 evolving threats and challenges of cyber.

For a small business, the consideration to add a security team often was not even on the table before the pandemic. With everyone working in a central location, their small IT team could secure the network easily. With everyone remote, this is not an option, and hackers know it.

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, making them a perfect target for ransomware attacks requiring victims who were not prepared to pay the ransom to restore business operations.

THE CYBER LANTERN APPROACH

One of the biggest benefits of hiring an external team to help manage your security is that you get the talents of a team for less than the cost of a single employee. Unlike building your own team, the 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 give you state of the art security at affordable costs. Employing an in-house team of your own may seem nice but can be resource intensive and lead to high operational costs to maintain a basic 9 to 5 operation.

CYBER LANTERN: THE COST OF SECURITY SERVICES

SECURITY OPERATIONS COST BREAKDOWN

While the cost of running security operations can vary greatly depending on several aspects, generally SMBs can expect to incur annual costs for tool licenses, infrastructure costs and human resources. When you hire the Cyber Lantern team, the cost of human resources is significantly lower. as you get more resources with greater knowledge. 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.

	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***

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 & new)
- ✓ Brand reputation
- ✓ Time to remediate
- ✓ Ransomware payouts
- ✓ Incident Response
- ✓ Brand reputation

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.