LOGO

Company Name
Address
City, State ZIP
URL: www.domain.com

[INSERT BUSINESS NAME]
[INSERT BUSINESS ADDRESS]

To [INSERT CUSTOMER CONTACT NAME],

As your IT partner, we have important information to share about an emerging threat that requires immediate attention.

The cyber security landscape continues to evolve at an astounding rate. In the past 12 months alone there has been a 715% increase in ransomware attacks. These ransomware attacks impact businesses every 11 seconds with 30% of all breaches impacting small businesses. Increasing regulations also make it imperative that businesses proactively secure their digital assets and network infrastructure.

Attackers are organized, well equipped and agile in their approach to find an open door to exploit systems and extract large ransoms. The average ransom a company pays has grown from $84K to $234K in the past 12 months alone and that number does not include any losses due to downtime, lost productivity or lost revenue. In fact, the average downtime for a business following a ransomware attack is 19 days.

Unfortunately, it is no longer a question of if you are going to be attacked, but when, how often and are you resilient enough to survive. As the threat landscape has grown and evolved, we have consistently had to evolve as well to keep our customers protected. As your trusted technology partner, we have reached a point where additional immediate action is now warranted.

Upgrading your cyber defense. **<<<MSP NAME>>>** has always been focused on security. Our approach is rooted in risk management—we adapt our processes and technologies on today's threat landscape, adding the appropriate layers of protection for our clients. Below are the recommended standards that we advise all clients should be consuming as a base level of security.

- Proactive Patching, Alerting and System Management
- Integrated and Intelligent Perimeter and Endpoint Security
- Microsoft Cloud Security Advanced Threat Protection
- Identity Security with Multifactor Authentication (MFA)
- Security Awareness Training & Programs
- On Premise & O365 Backups and Disaster Recovery Services

These layers have evolved over time and have arrived at a point where additional services are requires to provide your business the right level of protection. Along with this, many cyber-insurance providers are starting to reward investment in these kind of tools, or also penalize organizations that aren't.

Ultimately, we are making changes to increase the level of protection you receive from us as a way to enhance your security posture and reduce the risk of breaches and ransomware.

Security Operations Center (SOC). **<<<MSP NAME>>>** will be continuing to invest in our goal to create one of the most secure client communities in **<<<STATE/LOCATION>>>**, by augmenting the Sophos Intercept X Platform with the Sophos Managed Detection and Response (MDR) Service. We've worked very closely with Sophos to create a joint venture to manage active threat responses. The continuing emergence of human-led attacks require a combination of AI/machine learning products and human-led threat hunters to effectively combat the growing risk. Our SOC will take all of the security information between the endpoint devices and network firewalls to actively monitor for threats – including proactive hunting for insider threat activity.

What does this change mean for you? On **<<<ROLL OUT DATE>>> <<<MSP NAME>>>** will be rolling out these changes across the entire **<<<MSP NAME>>>** Managed Services Community. This will ensure that each network we manage has the same level of cybersecurity protection regardless of its size or complexity. **<<<MSP NAME>>>** will take on the majority of the cost to upgrade and deliver these new protections. However, clients will see an increase to the following managed line items:

[insert line items]

We understand that every business is different, but our experience has taught us that this risk needs to be taken seriously across the whole client community. If you have questions about this change or would like to complete a more thorough review of your current security posture, please reach out to your **<<<MSP NAME>>>** Account Team or Service Delivery Manager.

Thank you for trusting in **<<<MSP NAME>>>** to provide your business with a superior level of support and the cybersecurity protection it needs!

Regards,

SIGNATURE

Name
Title
Company Name