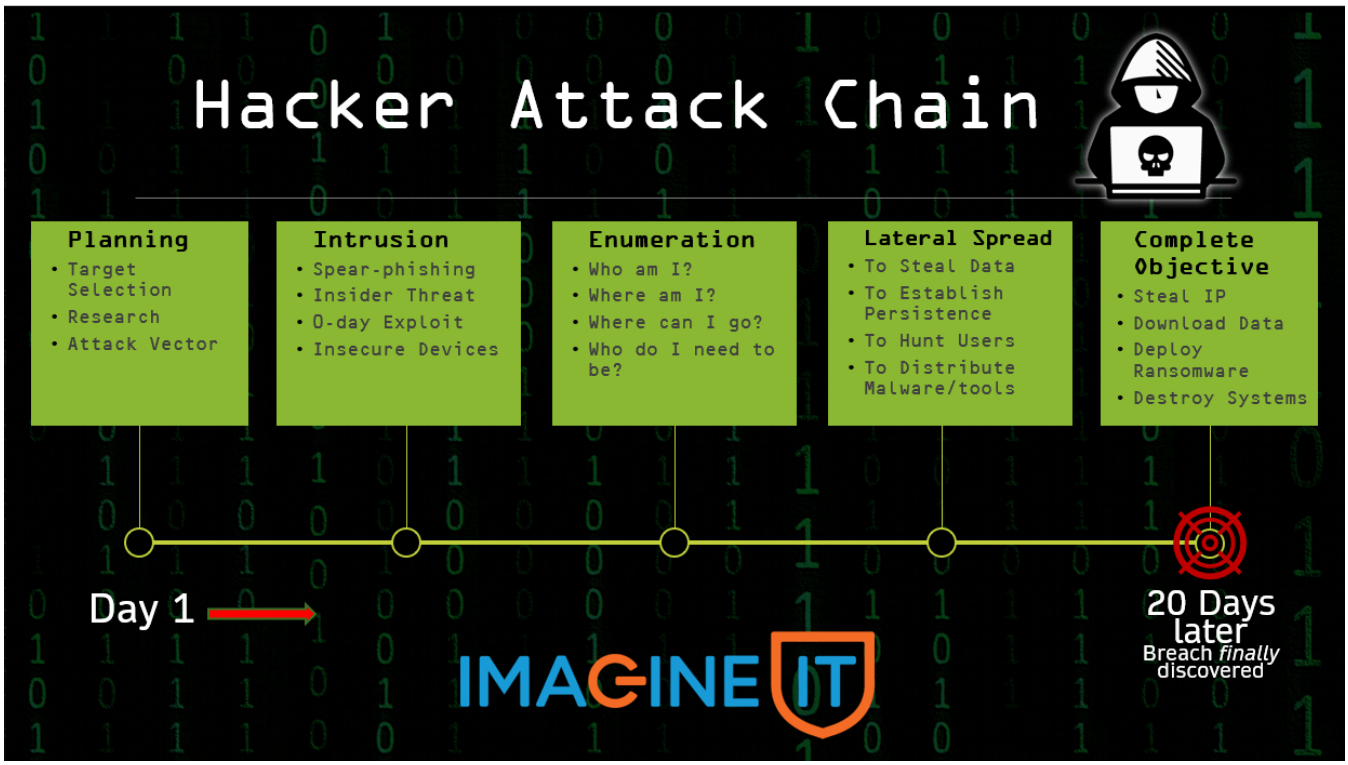
Security Shield Enrollment Proposal

City of Bel Aire

Prepared by: Peter Durand
Imagine IT, Inc.
November 2023

Overview

Cybersecurity is not an IT problem, it's a BUSINESS problem that impacts all departments. Unfortunately, the world has changed and traditional security technologies like firewalls, antivirus, VPN, and passwords are no longer enough. Breach tools and processes have become widespread and commoditized, and it's now just too easy for cyber-criminals to gain a foothold in business environments. Here is how hackers successfully compromise businesses...



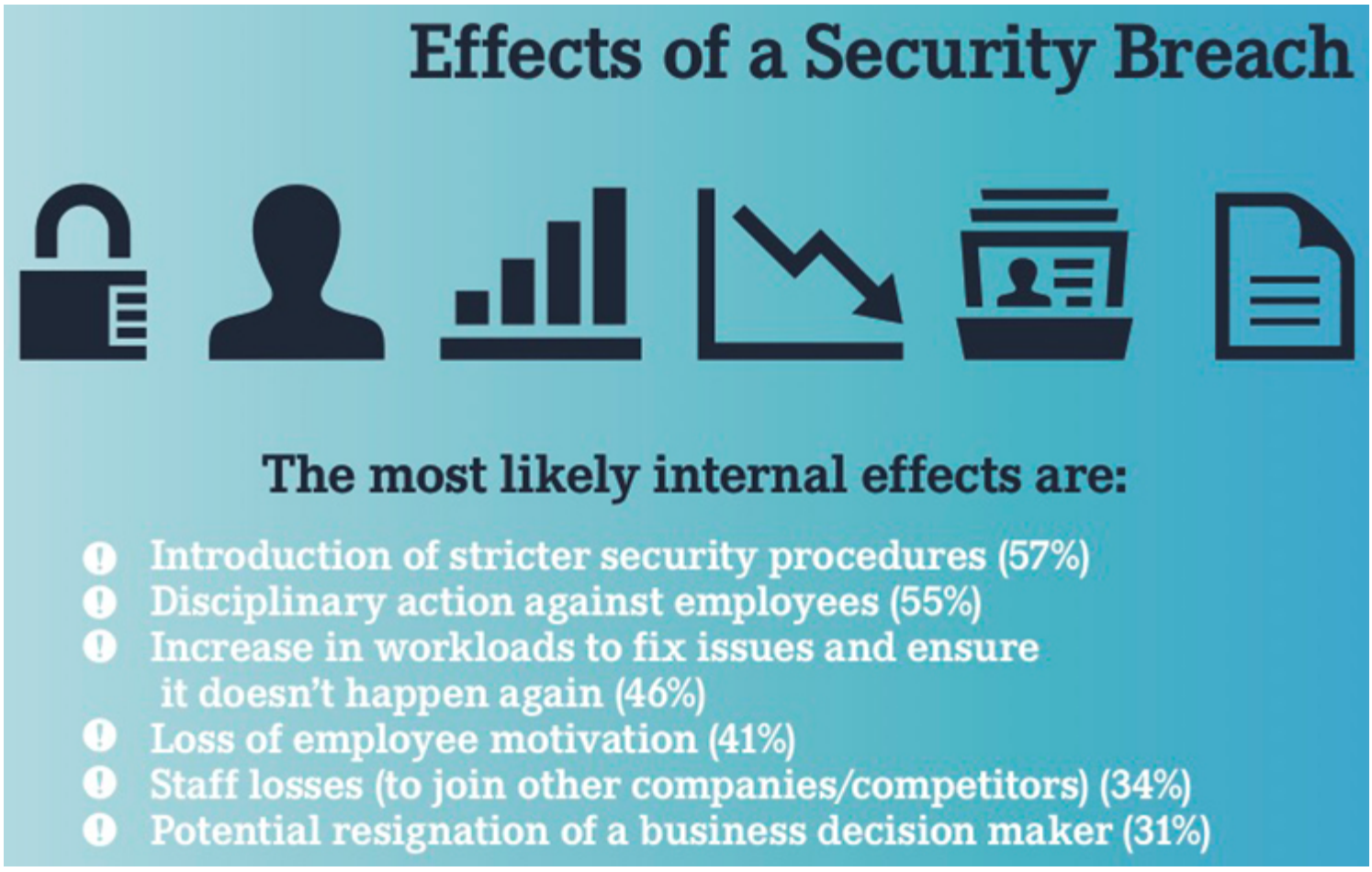
According to the [2023 Diligent Institute survey of "What Directors Think",] board members ranked **cybersecurity as the most challenging issue to oversee**, ahead of digital transformation, innovation, new technologies and capital allocations.

The Critical Questions

Boards and executives need to be able to answer these critical questions…

- What are our most important assets and how are we protecting them?
- When will the attack come?
- Is the business prepared to detect it?
- Is it prepared to stop it?
- Can it mitigate the effects and get back to normal operations as quickly as possible?
- What will be the impact of the breach?
- If we become a victim:
    - Why did we wait to prioritize investments in cybersecurity?
    - Who is going to be held accountable?

The Executive Team must have a plan and prepare the entire organization for the eventuality of an attack. The question is not whether the attack is going to happen and how to prevent it.

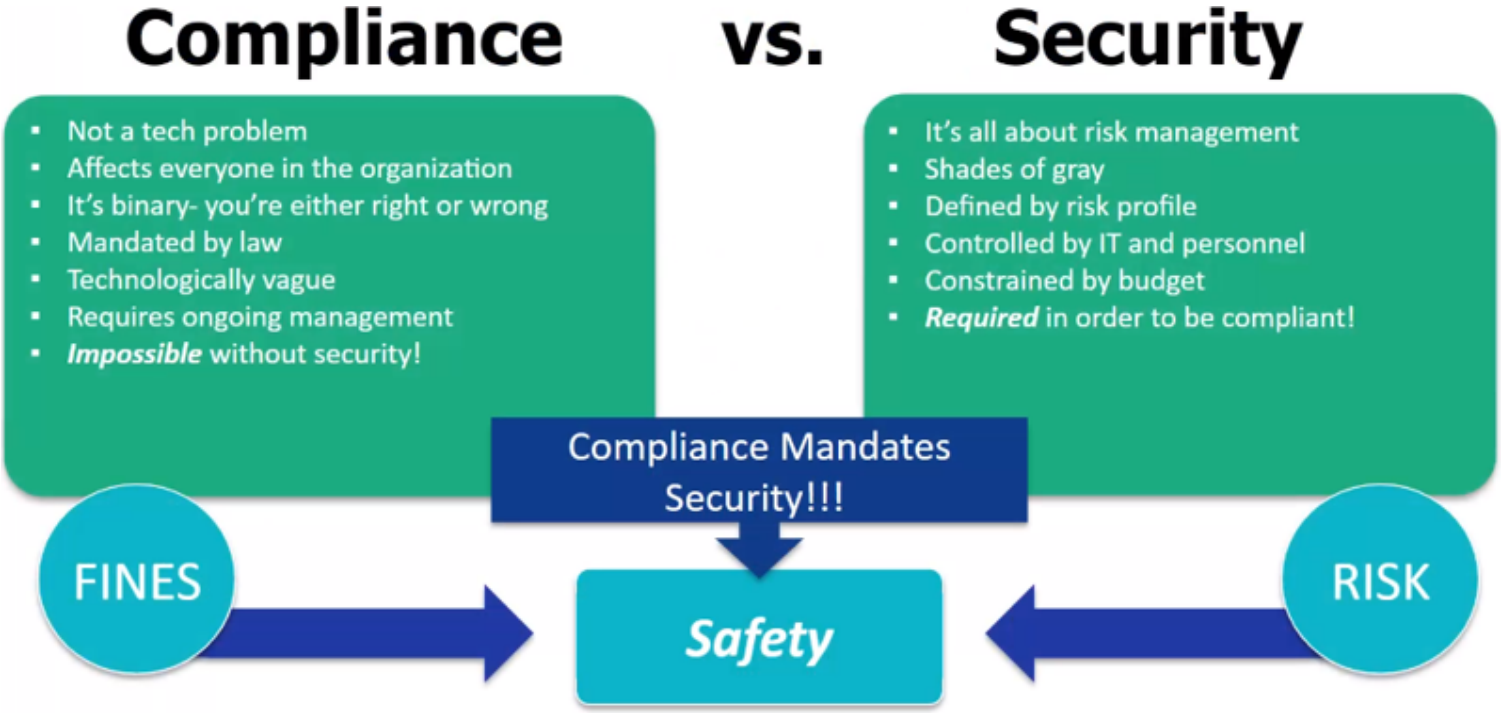


Cyber Insurance Requirements

Municipalities desire affordable cyber insurance. However, the insurance companies recently made qualifying MUCH more difficult, requiring businesses to maintain a security posture well above typical levels. It will be virtually impossible to qualify unless enrolled in a comprehensive and modern Managed Security program that can cover all the requirements.

Lloyd's of London recently announced they will no longer cover state-sponsored attacks. Other carriers will follow. What does that mean to your business? It is even more critical to avoid a serious breach.

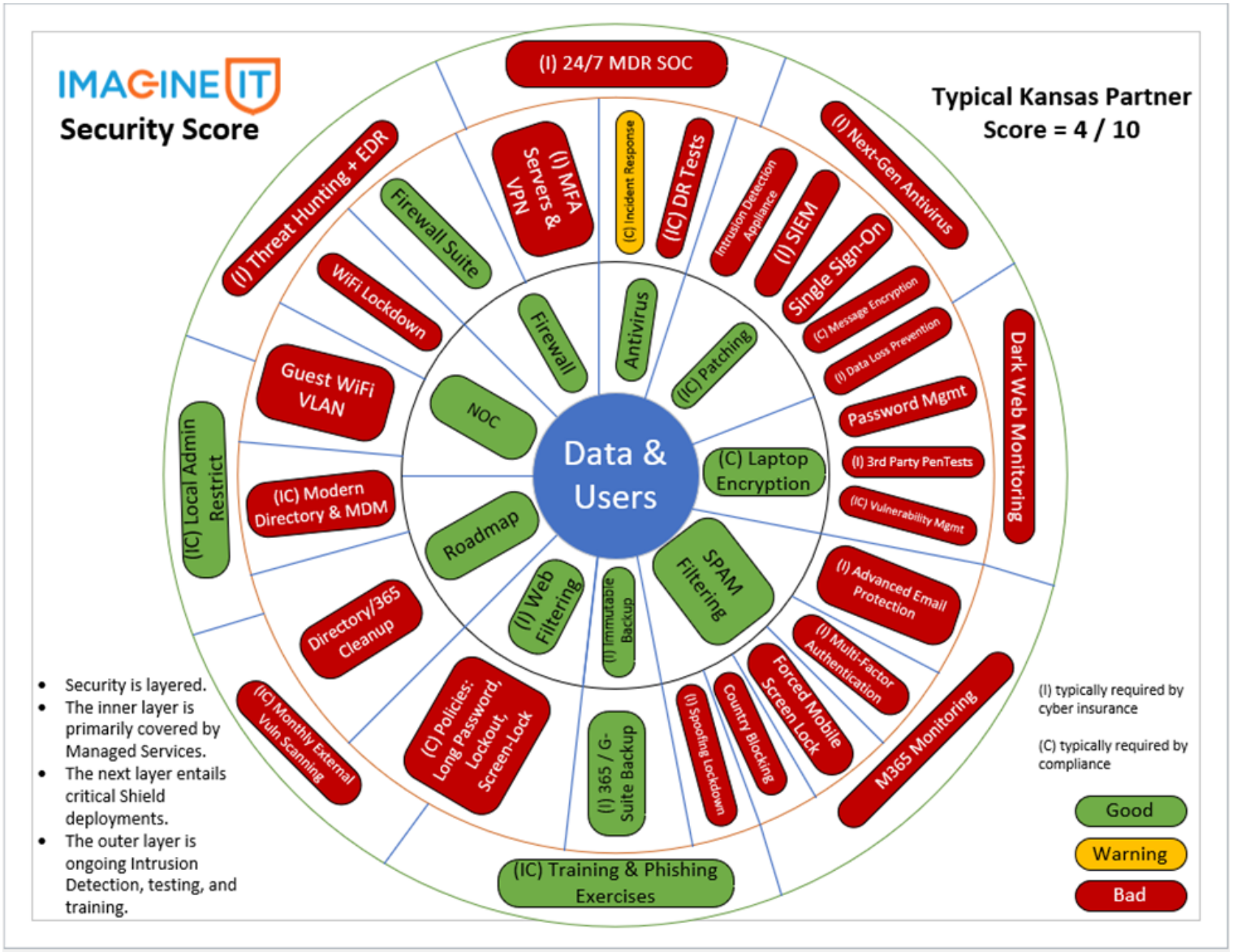
Compliance DOES NOT EQUAL Security



Current Security Posture

As you think about how skilled the cyber-criminals have become, and place that into the context of your current security posture represented below, it should become clear that it's only a matter of time before a breach takes place. And to be honest, you are bringing a knife to a gunfight, and we just can't protect you any longer with decades-old security practices. The ONLY way to protect your data and livelihood is to enroll in a robust Managed Security program, that for **roughly $1/day/employee can protect THOUSANDS in daily revenue**.

Oh you have backups and insurance? Can you restore your reputation and business valuation? Or retrieve your Intellectual Property or confidential client information from the Dark Web? How long will it take to rebuild ALL endpoints after a broad Ransomware attack?



3 Month Target Security Posture

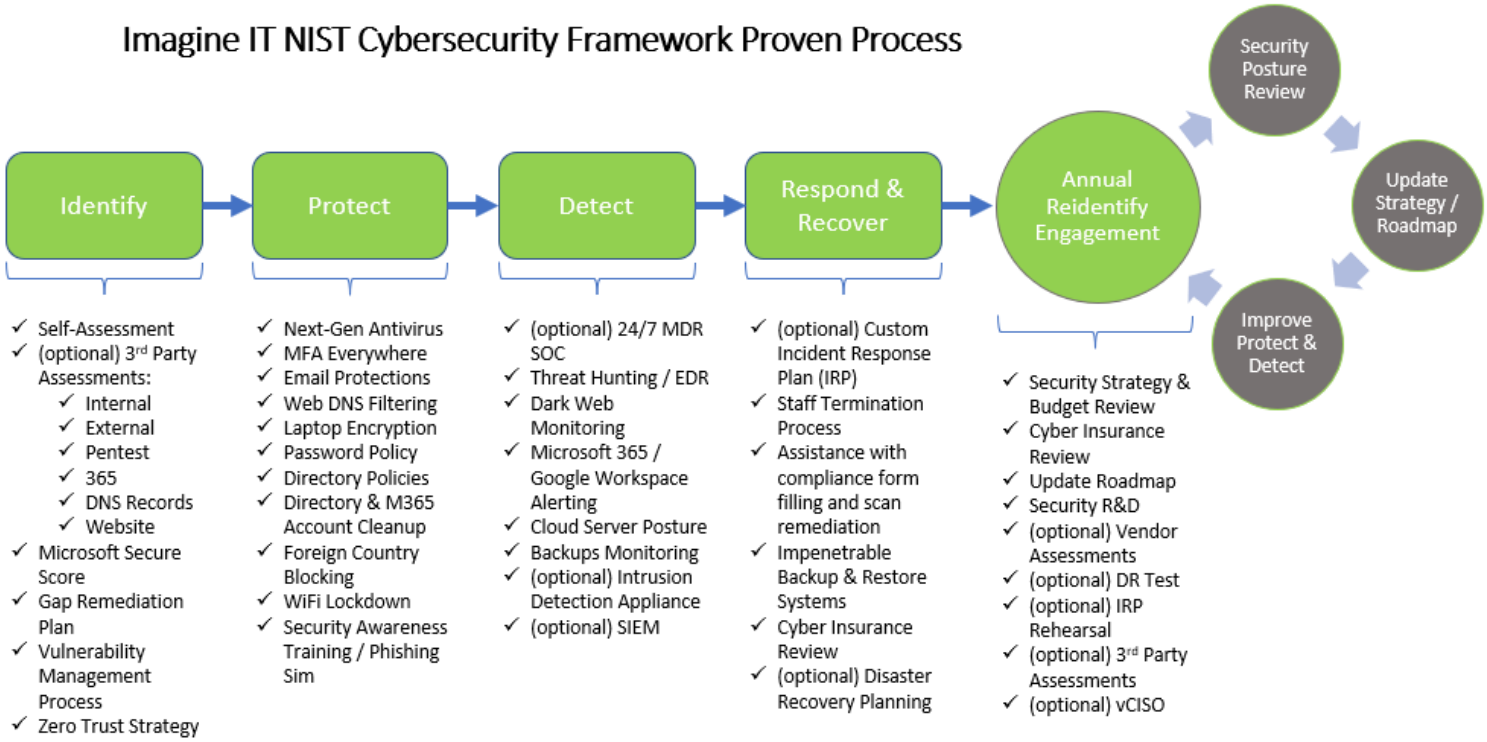
Deploy "Modern Security" solutions and processes to protect, monitor, investigate, and provide recurring user training. We call this "The Shield". The Shield is designed around the "Zero-Trust" model (assume breach, verify user, only access from approved devices) and the 5 pillars of the National Institute of Standards and Technology (NIST) Cybersecurity Framework:

- **Identify:** Document the current gaps and make a remediation plan and timeline.
- **Protect:** Deploy technologies that avoid breaches.
- **Detect:** Deploy technologies that detect breaches (assume there will be breaches).
- **Respond:** Document a thorough Incident Response Plan, and rehearse it annually. Imagine IT has this.
- **Recover:** Deploy bullet-proof backup solutions, Cyber Insurance, and document a Disaster Recovery Plan.

Address "Cyber Resilience" (post breach remediation planning), not just "Cyber Security" alone (preventing breaches).

In short, we will:

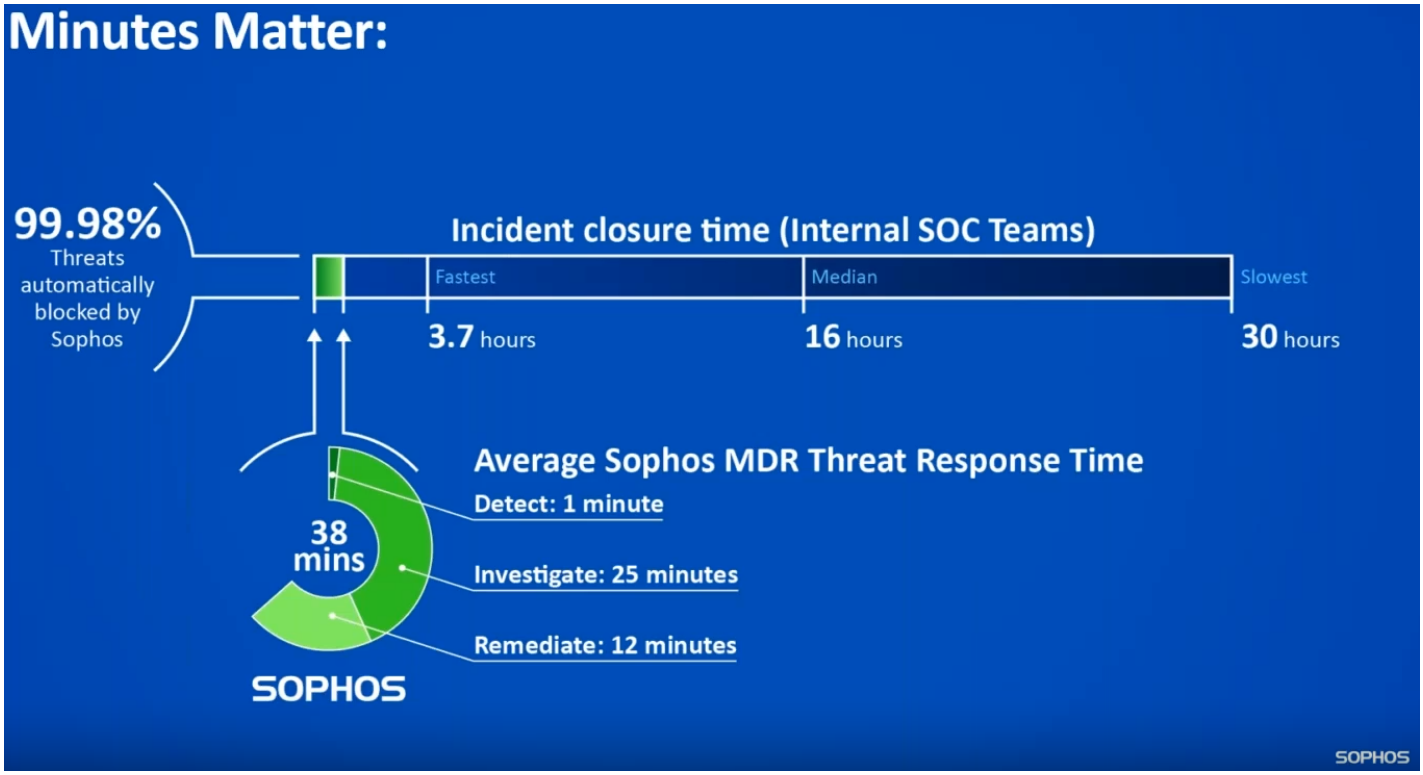
- Lock it down
- Train your users (95% of breaches are caused by human error)
- Monitor for breaches
- Continually improve your security posture
- Make security a competitive advantage
- Protect reputation, revenue and business valuation



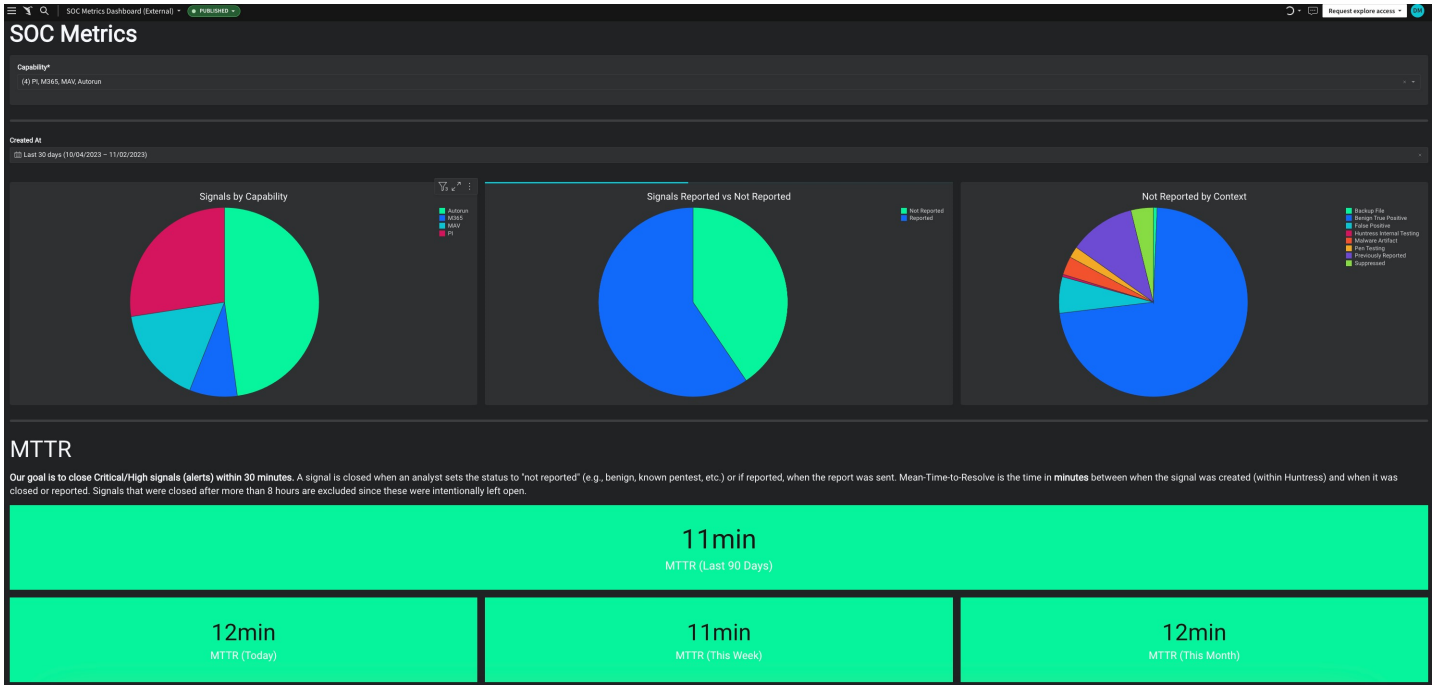
Blazing Fast Neutralization

The typical business Security Operations Center (SOC) average time from detection to neutralization = 16 hours (much too late).

The Imagine IT SOC average time from detection to neutralization = 11 minutes (hacker stopped).



Huntress SOC = 11 Minutes Average



Shield MDR Magic Quandrant

G2 MDR Magic Quadrant

Huntress and Sophos are both upper right…

Shield "Essentials" Program Monthly Costs	Recurring	Qty	Ext. Recurring
Security Shield Essentials (62 email users, 77 devices)	$1,580.00	1	$1,580.00

- Initial One-Time Protections (Email Security & MFA, WiFi Lockdown, etc…).
- Next-Gen Antivirus Management.
- 24/7 MDR Security Operations Center (SOC). **Often required by cyber insurance.**
- 24/7 Human-Led Neutralization.
- Proactive Threat Hunting.
- Breached Device Isolation.
- Recurring Security Awareness Training / Phishing Simulations.
- Dark Web Monitoring.
- Monthly Vulnerability Scanning (external only).
- Cyber Insurance Form-Filling Assistance (remediation billed separately).
- Compliance Form Filling Assistance for PCI-DSS and HIPAA (remediation billed separately).
- Imagine IT Incident Response (up to 10 hrs/incident).

Monthly Subtotal:	**$1,580.00**

Microsoft 365 Security Subscriptions	Recurring	Qty	Ext. Recurring
Microsoft Defender for Office 365 GCC (Plan 1) Monthly	$2.40	62	$148.80
Microsoft Defender for Cloud Apps [NCE] Monthly	$4.20	62	$260.40
		Monthly Subtotal:	**$409.20**

Shield Statement of Work - Fixed Fee

This Statement of Work (“SOW”) is an addendum to the Master Service Agreement, dated April 1, 2023 ("MSA”) is between Imagine IT (“Imagine IT”) and (“Client”). Any capitalized terms used herein shall have the meaning given them in the MSA.

1. Scope. The services to be provided by Imagine IT by this SOW shall be as follows. Imagine IT shall perform:

Phase 1

- **Threat Hunting / EDR**
  - Without this, we cannot detect malicious activity that may have bypassed the antivirus or firewall.
- **Dark Web Monitoring**
  - Without this, we will not get alerted and cannot take action if a user's credentials are exposed.
- **Next-Gen Antivirus**
  - Without this, we cannot detect and take action on advanced types of malware and ransomware.
- **Vulnerability Scanning Platform (External Only)**
  - Without this, vulnerabilities may not be detected until it is too late.
  - Customer will be required to assist with much of the remediation, especially user applications.
- **Microsoft Defender for Office 365 (Plan 1)**
  - Without this, malicious links and attachments are more likely to make it into user mailboxes.
- **Microsoft Defender for Cloud Apps**
  - Without this, we may not get alerted to suspicious activity until it is too late.
- **(done) Microsoft 365 Backup**
  - Without this, it may be challenging to recover from an Office 365 breach, file loss, or corruption.

Phase 2

- **Microsoft 365 Phone/Tablet Inactivity Screen Lock**
  - Without this, a lost cell phone could expose confidential data and/or lead to a larger breach.
- **Microsoft 365 Block Email from Known Suspicious Countries**
  - Without this, users will be exposed to more SPAM and phishing.
- **Suspicious Country Blocking for Firewalls (best effort if not IIT Stack Firewall)**
  - Without this, hackers outside the U.S. can try to hack through your firewall.
- **Spoofing Email Lockdown of SPF/DKIM/DMARC records**
  - Without this, a skilled hacker could send messages with the exact spelling of your domain name, and legitimate outbound messages are more likely to end up in quarantine.
- **Spoofing Email Lockdown by enabling an "External Sender" banner**
  - Without this, it makes it more difficult for a user to spot an email imposter.
- **Directory & M365 Account Cleanup**
  - Without this, inactive account users and/or common usernames with weak passwords may lead to a breach, as do active users with Admin privileges.

Phase 3

- **Microsoft 365 Multi-Factor Authentication (MFA)**
  - Without this, a hacker can gain access to a mailbox and other 365 data and settings once they obtain the password.
- **(done) Recurring Security Awareness Training**
  - Without this, users will be more likely to make mistakes that could lead to a breach.
- **Long Password Policy**
  - Without this, powerful hacking tools can guess passwords very quickly.
- **Computer Inactivity Screen Lock**
  - Without this, a hacker could obtain access to a computer and confidential data.
- **(done) User Local Rights Lockdown**

- Without this, users can install unapproved applications, including malware.
- **Change WiFi WPA2 Password to a long Phrase**
  - Without this, it is fairly easy for a nearby hacker to get on the network.
- **Setup Guest WiFi VLAN (only for IIT Stack Switches and Access Points)**
  - Without this, a compromised cell phone could expose the network to malicious activity.

After Completion

- **Perform the Group Security Awareness Training Webinar (if approved).**
  - Without this users may fall for social engineering tactics.
- **Kickoff the 3rd Party Penetration Test (if approved).**
  - Without this, you may not be made aware of uncovered security vulnerabilities until it is too late.
  - Remediation is out of scope.

2. Fees. Client hereby engages with Imagine IT on a Fixed Fee basis in the amount listed below. Progress billing will be sent monthly until completion of the Services.

3. Client Obligations.

- Cooperate with Imagine IT in all matters relating to the Services and appoint an employee to serve as the primary contact with respect to the Services and who will have the authority to act on behalf of Client with respect to matters pertaining to the Services.
- Provide Imagine IT with reasonable access to Client's environment as may reasonably be required by Imagine IT for the purposes of performing the Services;
- Respond promptly to any Imagine IT request to provide direction, information, approvals, authorizations, or decisions that are reasonably necessary for Imagine IT to perform Services;
- Obtain and maintain all necessary licenses and consents and comply with all applicable Law in relation to the Services, the installation of the Imagine IT Equipment (if any), the use of Client's materials, and the use of the Client equipment.

4. Exclusions & Additional Terms

- This SOW does not provide any terms or conditions associated with the purchase of Product, which shall be by a separate Addendum.
- The cost to bring Client's System up to minimum standards required to perform Services.
- Any Services related to the above are beyond the scope of Services and shall be on a time and materials basis in accordance with Imagine IT's standard rates together with Imagine IT's actual expenses. Imagine IT shall issue invoices to Client monthly in arrears for fees outside of Scope, together with a detailed breakdown of time, materials and expenses.

The Term of this SOW shall not be in accordance with the defined term for SOW's in the MSA but shall be until completion of the Services. This SOW is effective upon execution by Imagine IT and Client. Each party hereto warrants and represents that this SOW and the MSA constitute the legal, valid and binding obligation of such party as of the date signed by Client below ("SOW Effective Date").

Shield Deployment Upfront Costs	Price	Qty	Ext. Price
Security Shield Deployment Labor	$6,000.00	1	$6,000.00
		Subtotal:	**$6,000.00**

Customer Requirements

- Security is a shared responsibility. Executives have a role. Managers have a role. End-users have a role. It doesn't work if everyone isn't on board and doing their part.
- Everyone that has an active mailbox must be included.
- All business owned computers must be included.
- We will exclude lab/student/dev nodes from Endpoint Protection deployments.
- Excludes investigation/remediation work related to home or non-included computers, websites/ecommerce, or other systems outside of the Shield protection capabilities.
- For global-scale attacks, IMAGINE IT Security Shield partners will be first in line for incident response.
- Customer must maintain Cybersecurity Insurance ample enough to cover ransomware payments, recoup lost revenue, recovery expenses, and reputation harm, caused by breach or cyber-deception.

Future Shield Upgrades Policy

The cybersecurity landscape continues to change rapidly. Unfortunately, nation states and organized cyber-crime are getting stronger at an exponential rate, largely because they are sharing/selling their knowledge and services to each other. These criminals have proven their capabilities to exploit, exceed the skill level of our public and private sectors to protect. We are literally in a cyber-war with no end in sight.

Our strategy is to proactively stay ahead of the hackers, and to do that requires continual R&D and periodic improvements to The Shield. Therefore, we plan to improve the Shield 1-2 times per year and include newly added protections and potential removal of others. Our goal is to continually improve protection while keeping cost close to the same or with only small increases.

As each Shield improvement is released, your org will automatically be enrolled. If there is upward price impact, we will provide written notice 30-days in advance.

Scope Change Process

Scope Change Requests frequently occur during projects due to the dynamic and collaborative nature of project execution, even if there was significant due-diligence. The following process will be utilized if a change is identified which materially affects the scope described in this proposal:

1. Imagine IT will generate a Scope Change Request describing the identified change, the number of hours required to affect the change, any additional charges, and the timeline.
2. Upon signed approval by the customer, the work will be scheduled and performed.

Project Success Agreement

Imagine IT agrees…

- To complete Phase 1 within 2 weeks of the project kickoff date.
- To simultaneously execute the remaining two phases and complete them within 4 weeks after completion of Phase 1. However, Phase 3 is highly dependent on Client adherence to their commitments (see below).

Client agrees…

- To provide Registrar & DNS account access within 1 week of signed project approval.
    - Imagine IT requires admin accounts setup that we tie to our MFA.
- To assist with 365 licensing remediation (inactive users, etc…).
- To cascade to users the upcoming changes on the required frequency.
    - Imagine IT will provide communication templates.
- To make ALL users available for user-facing deployments within 4 weeks after project kickoff:
    - Security Awareness Training.
    - Password Policy changes.
    - MFA enrollments.
    - WiFi changes.
- To assist users with their deployments and be the frontline for initial user support requests.
- To at least quarterly login to the Sophos portal and review user compliance.
- Recurring billing starts when Phase 1 is complete.
- If Client delays Phase 3 commitments:
    - Client may lose their place in the Imagine IT project queue and there could be a significant delay in project completion, creating risk to Client.
    - Client may be on the hook for additional deployment costs for Imagine IT to remediate delayed tasks.

Security Shield Enrollment Proposal

Prepared by:

Imagine IT, Inc.
Peter Durand
952-905-3710
pdurand@imagineiti.com

Prepared for:

City of Bel Aire
7651 E Central Park Ave
Bel Aire, KS 67226-7600
Ted Henry
(316) 744-2451
thenry@belaireks.gov

Quote Information:

Quote #: 010406
Version: 1
Delivery Date: 11/30/2023
Expiration Date: 12/31/2023

Quote Summary

Description	Amount
Shield Deployment Upfront Costs	$6,000.00
Total:	**$6,000.00**

Monthly Expenses Summary

Description	Amount
Shield "Essentials" Program Monthly Costs	$1,580.00
Microsoft 365 Security Subscriptions	$409.20
Monthly Total:	**$1,989.20**

Recurring MSP Agreement invoices are due on invoice date; all others NET 15 days. Hardware is invoiced upon receipt; project progress billing is sent monthly. Taxes, shipping, handling and other fees may apply. Leasing options are estimated. Imagine IT reserves the right to cancel this proposal due to pricing change or product availability at any time prior to acceptance by both parties. All products are custom ordered. If client wishes to return, cancel or change products after proposal acceptance, a restocking fee equal to 10% of returned products, excluding sales tax, will be assessed. Returns for defective products must be made within 30 days of delivery. The products proposed herein are subject to the manufacturer's warranty. Imagine IT does not warrant any products against manufacturer defect.

Imagine IT, Inc.

Signature: Peter Durand
Name: Peter Durand
Title: CTO
Date: 11/30/2023

City of Bel Aire

Signature:
Name:
Date:
PO Number: