VIMRO
OUTCOME AS A SERVICE

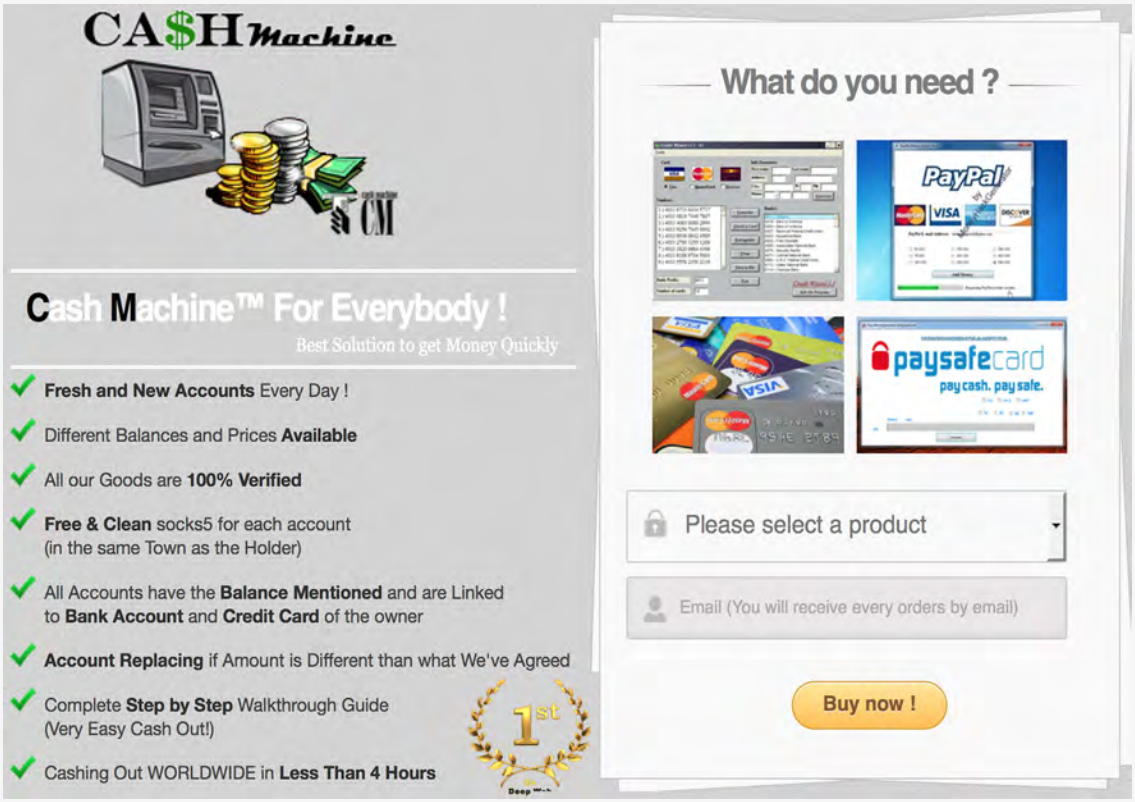
Dark Net
The Devil is in the Details

"At their core these sites are meant to serve one purpose: enable privacy and free speech...."

Just like Lucifer, the Dark Net is known by many names with only subtle differences in meaning: the Dark Web, the Digital Underground, and the Deep Web, to name a few. Dark Net sites are difficult to find because they do not show up in normal search engines, but they are accessible through TOR or Tails. At their core these sites are meant to serve one purpose: enable privacy and free speech on the Internet. Unfortunately, they also provide fertile ground for illegal activities, such as selling contraband drugs, firearms, and stolen data, as well as much worse crimes.

When you hear a news story about yet another data breach, you can be confident the stolen data will be available on the Dark Net, on information brokerage sites known as Dark Markets. Some of these Dark Markets trade in stolen data (credit cards, Social Security numbers, personally identifiable information, protected health information, and so forth). Figure 1 below depicts a Dark Market welcome page offering bank account information; and Figure 2 displays a list of prices for chipped and magnetic-only credit cards.

Figure 1 – Screenshot Example of an Illegal Dark Market Site

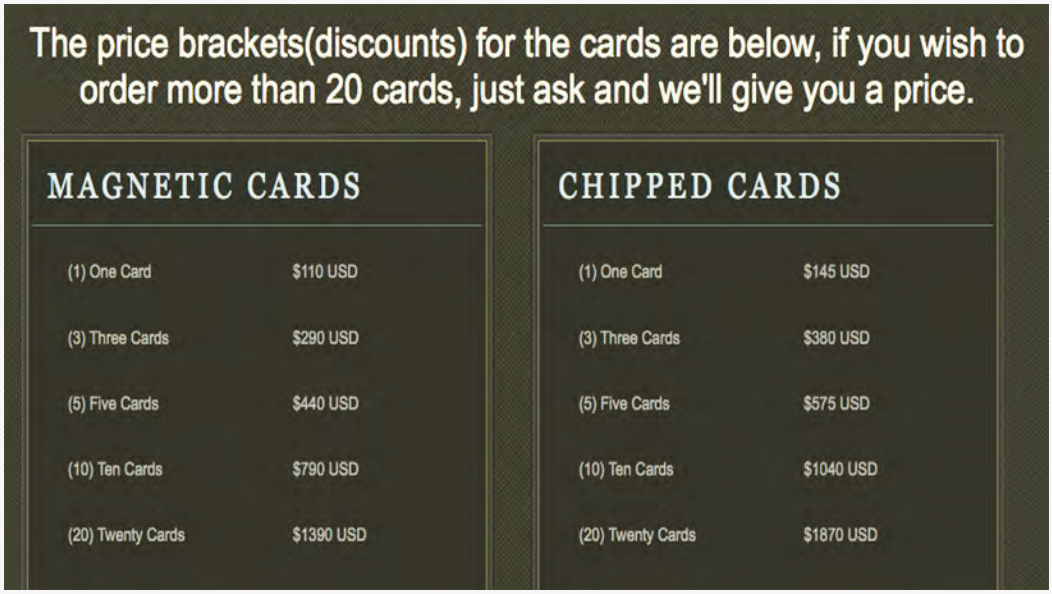


Dark Net
The Devil is in the Details

VIMRO
OUTCOME AS A SERVICE

> "The Dark Market has made it easy for criminals without hacking skills to get what they want....."

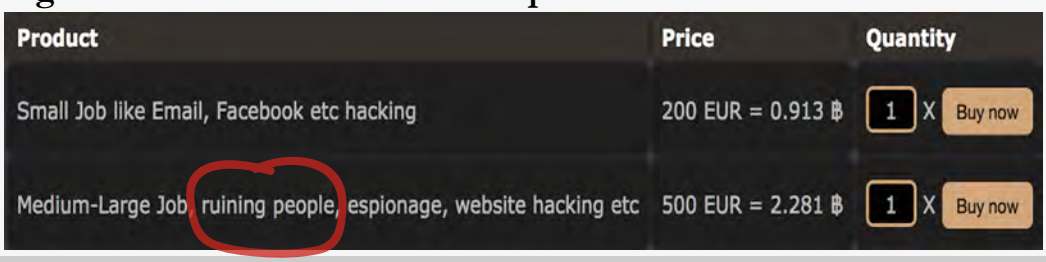
Figure 2 – Screenshot of an Illegal Dark Market Pricing Page



VIMRO security team members are often asked, "Why would a criminal want our data and how could they use it?" Criminals want whatever data we have, and they will find a use for it all. It may seem insignificant at first glance, but each bit of data (email accounts, social media accounts, passwords, birthdays, mothers' maiden names, addresses, workplaces, prescribed medications, and so on) can add up to be worth $1,000(1) in a Dark Market; and the more data available on one individual, the more money that data is worth to Dark Market dealers.

The Dark Market has made it easy for criminals without hacking skills to get what they want: they simply hire someone to do the dirty work for them. Hackers for hire wait on the Dark Net, ready to commit various Internet crimes for the right price. This makes all organizations — and individuals — potential hacking victims. Figure 3 is an example of one hacker's service menu.

Figure 3 – Hacker for Hire Example



Dark Net
The Devil is in the Details

"As aggrressivly as the FBI infiltrates and shuts down Dark Market sites, MORE sites spring up."

Some of these criminals are willing to do whatever the buyer asks, such as perform DDOS attacks, corporate espionage, hacktivism, and so forth. And it's easy and simple to pay for these crimes! You may have noticed the ฿ symbol in the Price column of Figure 3. This is one of the symbols for Bitcoin[2], whose guarantee of anonymity for both buyer and seller has made it the common currency of the Dark Market.

The Dark Net has made cybercrime seem safe and easy, and there is no permanent solution in sight, at least in the near future. For law enforcement, this means a repeating cycle of stopping one cybercriminal ring only to move onto the next. As aggressively as the FBI infiltrates and shuts down Dark Market sites, more sites spring up.

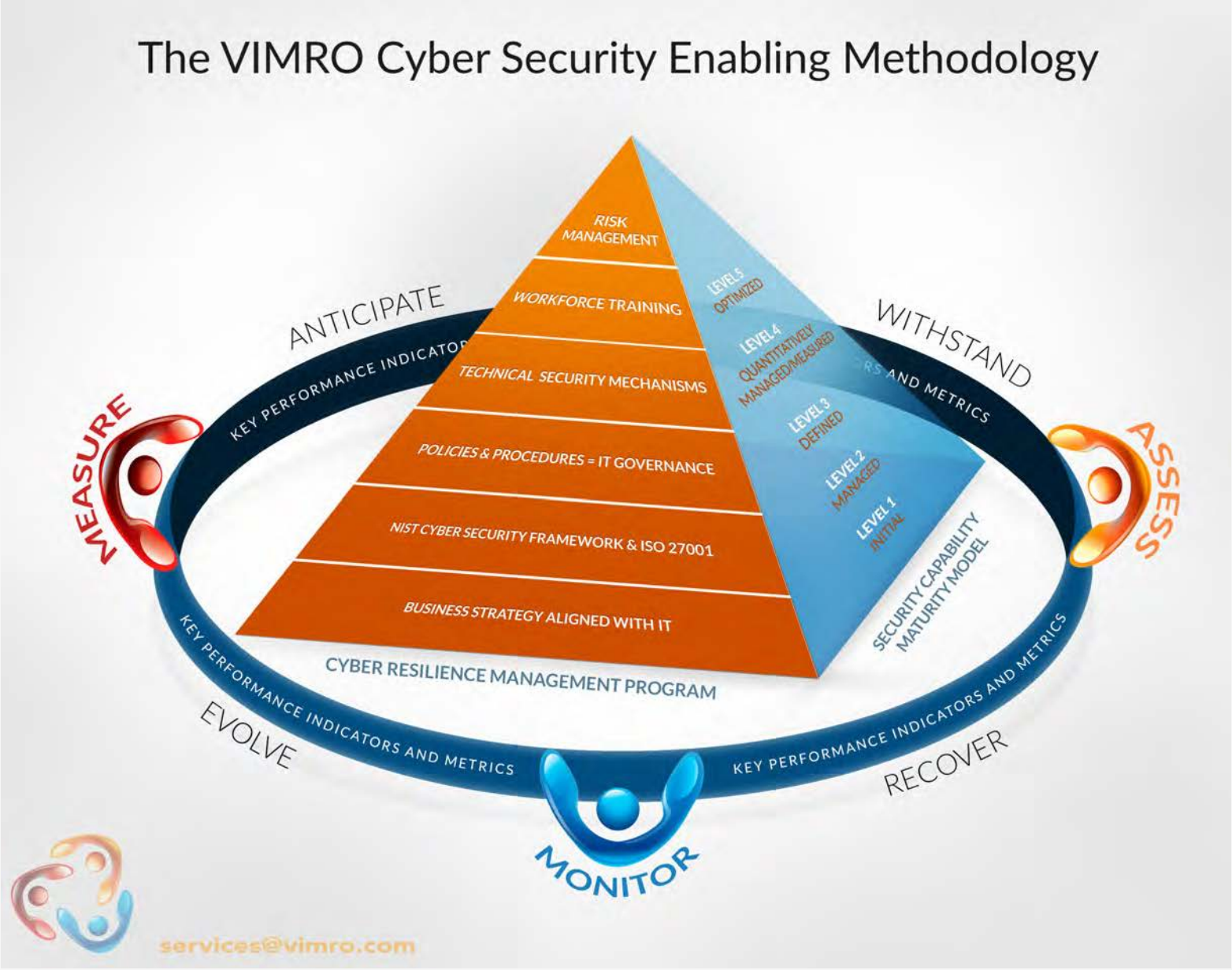
To protect your company, your employees, and your customers from cybercrime in this volatile environment, you must invest in a good cyber security program. VIMRO's approach is a holistic security methodology that includes the elements in Figure 4.

[1] Example of Identity Prices in the Dark Market: http://www.networkworld.com/article/2880366/security0/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html
[2] Bitcoin Wiki: https://en.bitcoin.it/wiki/Main_Page

Implementing quickly or without adequate resources will dangerously reduce effectiveness.

Note that for our methodology to succeed, you must adopt it in a controlled manner and treat it as an evolving process. Implementing it too quickly or without adequate resources may reduce the security program's effectiveness and demotivate the team members involved. Here's an overview of a VIMRO cyber security system:

Figure 4 – VIMRO's Cyber Security Enabling Methodology



Dark Net
The Devil is in the Details

The methodology assures the organizations business needs align with your security requirements.

- The foundation of our security system first aligns your organization's business needs with your IT security, allowing you to focus on the critical business applications, systems, and processes that need strong security controls. For example, when you implement a new application, include a security representative in the development of the budget and project plan. This way, you are assured that time and resources are allocated for security controls throughout the project; and for support throughout the new application's lifecycle. If you overlook security requirements in the beginning stages of a project, the application and associated systems may require rework for failure to meet your company's approved security standards. And rework, delays or budget excesses invariably reduce your new application's ROI.
- The second layer of our foundation includes implementing a security framework. Many of VIMRO's clients have adopted either the NIST(3) Cybersecurity Framework or ISO27001/ISO27002(4).
- Along with the framework, organizations have adopted a cyber security Capability Maturity Model (CMM) that provides a strategy to optimize critical security controls, mechanisms, and processes (Level 5 in the CMM). The cyber security CMM includes:
    - Level 1 – Initial: Processes are unpredictable, poorly controlled and reactive
    - Level 2 – Managed: Processes are characterized for projects and are still often reactive
    - Level 3 – Defined: Processes are characterized for the organization and are proactive, taking their procedures from the organization's standards
    - Level 4 – Quantitatively Managed: Processes are measured and controlled
    - Level 5 – Optimizing: Focuses on process improvement
- To manage performance leading toward the optimal level (Level 5) in the security CMM, we recommend Key Performance Indicator (KPI) metrics. Many clients start with MITRE(5) Cyber Resiliency Metrics.

(800) 272 0019

Ashburn, VA | Baltimore, MD | Boston, MA | Glendale, CA | Las Vegas, NV | Reston, VA | San Diego, CA | Tampa, FL

Dark Net
The Devil is in the Details

....the risk management program includes continuous evaluation of your mechanisms and process to validate them.

- VIMRO policies, standards, and procedures include all of the verbiage necessary to raise your organization to the upper levels of the cyber security CMM. These are critical to success. Without these, your organization will not even surpass Level 2 in the security CMM.
- After writing your security policies, standards, and procedures, we implement technological mechanisms to support your cyber security program, and train workforce members to apply the requirements of the formal documents to their practices.
- VIMRO's risk management program includes continuous evaluation of your technological mechanisms and processes to validate them, and find areas which need improvement, so that your company always maintains optimized security controls.

Below is an example application of the VIMRO methodology to one specific security control item: a firewall. The NIST Cybersecurity Framework includes Configuration Management in the family of controls. Using the firewall as our example:

- An organization includes firewall configuration requirements in a policy; procedures are written for how the firewall will be implemented and managed.
- The procedure includes a baseline security assessment vulnerability report. The baseline is to be updated whenever a change is made on the firewall.
- The policy, procedure, and baseline report define the controls (CMM Level 3) for the firewall.
- In order to determine if the company is maintaining controls for the firewall to meet CMM Level 4, the firewall is audited using KPIs (a common approach is to conduct firewall configuration audits every six months).

[3] NIST Cybersecurity Framework: http://www.nist.gov/cyberframework/
[4] ISO 27001/27002: http://www.27000.org/
[5] MITRE Cyber Resiliency Metrics: https://register.mitre.org/sr/12_2226.pdf

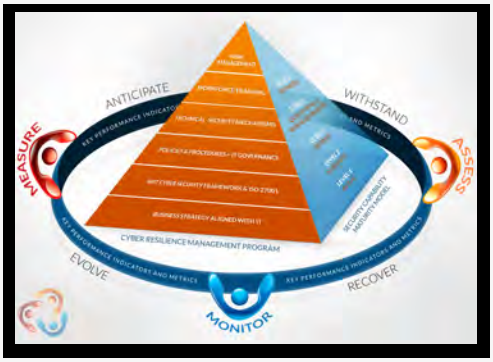
(800) 272 0019
Ashburn, VA | Baltimore, MD | Boston, MA | Glendale, CA | Las Vegas, NV | Reston, VA | San Diego, CA | Tampa, FL

Dark Net
The Devil is in the Details

A holistic and synergistic cyber security enabling methodology assures you and your organization reach the upper levels of the cyber security CMM.

- Some examples of KPIs include:
  - There must be a change record for each change made to the firewall. The acceptable KPI for changes without corresponding records is 0.
  - A vulnerability assessment report must not result in high or medium scores. The acceptable KPI for high or medium findings in a vulnerability assessment is 0.

- If during firewall configuration audits, some findings do not meet the KPI requirements, it is an opportunity to determine why this is the case. Perhaps there are too few people to meet the KPI objectives; perhaps skillsets are lacking and training on maintaining the firewall is necessary. For any items that do not meet KPIs, we implement a Corrective Action Plan (CAP), which sets expectation dates for the resolution of any issues cited. We conduct an audit immediately after said date to ensure that the items have been improved based on the CAP. This is an example of an optimized process (Level 5) for firewall controls practices.



Every layer of the VIMRO Cyber Security Enabling Methodology is critical for the success of an optimized cyber security risk management program. Systematic dedication to the process at each level assures a solid yet dynamic foundation proactively protecting you today and into the future. Based on this holistic approach, you can be confident that your cyber security initiatives will enable your organization to meet the needs to prevent, detect and respond to cybercriminal attacks that try to harm your business, clients, employees or steal your sensitive data.

Contact VIMRO to discuss the details of our cyber security enabling methodology, and learn how we help our clients streamline and realize their cyber security program initiatives.

(800) 272 0019
Ashburn, VA | Baltimore, MD | Boston, MA | Glendale, CA | Las Vegas, NV | Reston, VA | San Diego, CA | Tampa, FL