Cybersecurity White Paper

HARMONY TECHNOLOGY SERVICES
the power of harmony

ActiveCanopy

Now More Than Ever: The Heightened Need for Cybersecurity

Cybersecurity is not a one-touch, push-button, cure-all step to protecting your company's data. It's a well-planned process that begins with a detailed risk assessment of your company's needs. While some companies may purchase a high-level security package and feel satisfied that they've done all that they can, more and more companies are taking a smarter, risk-based approach.

The truth is no company can be completely protected—even when money is no object. In 2013, critical infrastructure companies spent a mind-numbing $46 billion on cybersecurity. Yet cyber-hacking continued to increase including notable incidents at highly protected corporations, such as Sony SPE, Anthem and Target. As a result, companies should focus on pinpointing their most vital data and to minimize the likelihood that it can be compromised by inside or outside threats. To achieve this, mindful companies are partnering with cybersecurity experts to protect their data based on an appropriate budget that includes firewalls, security software, cyber threat intelligence and human analytical efforts.

In this paper we will outline the proper steps to take to implement a dynamic cybersecurity system and why the uniquely robust partnership of Harmony Technology Services and Active Canopy™ can address these hardware, software and infrastructure foundations at a fraction of what competitors cost.

2015: Hackers Continue to Grow with Devastating Results

Less than two years ago, Black Friday became a cyber nightmare for 40 million Target customers when hackers stole their credit and debit card information from November 27 to December 15, 2013, the absolute height of

holiday shopping. Hackers had installed malware software right before Thanksgiving to steal the account information. What makes this landmark hack even more eye-popping is Target had already taken steps to prevent such threats by implementing FireEye, a $1.6 million (or multi-million dollar) malware detection tool used by government agencies. Even with a team of security specialists monitoring the computers around the clock, alarms about the security breach were missed. How? Human error. Although the detection tool had an option to automatically delete malware, Target's security team had turned off that function.

Though this may seem like an easily fixable problem in the future, considering the human element aspect of cybersecurity is a key lesson and focal point for implementing a firm grasp on its network security environment.

The Risks Are Great

As the Target data breach story reveals, companies of all sizes are at risk of having their data stolen. Hackers are getting more sophisticated every day and even though advances in cybersecurity continue to evolve, threats grow at an alarming rate.

Just as Sony SPE experienced, in the flash of a moment, hackers can destroy, manipulate or release to the Internet a company's:

- Personal data
- Intellectual property
- Trade secrets
- Network control and access
- Impact to operations if your network is disabled
- Image and customer relations
- And more

Should any of this information be compromised, your company could be devastated, go out of business and be subjected to lawsuits. It's a frightening reality that demands that you take aggressive steps now to implement well-structured, cohesive cybersecurity system.

What Type of Data Do Hackers Attack?

- Complex Data – such as health records
- BYOD (Bring Your Own Device) data -- attacking a device connected to a company's files and data
- Domain administrator's / Executive laptops / VPNs
- Connected Devices That Manage Large Scale Systems – critical infrastructures, such as water supply systems, traffic control systems, and train & subway switching systems
- Home/Office Networks & Automation – not only accessing home networks, but also system controlled locks, alarms and environmental controls as well as all of the "Internet of Things" (IoT) being connected every day
- Financial Data
- Intellectual Property
- Technology data
- Logistic, geo and image data to combine with human operations

Elements of Effective Cybersecurity

One of the first mistakes companies make when implementing cybersecurity is to believe that merely purchasing a data security package with firewall and software capabilities will do the job. This one-size-fits-all mentality can be fatal to your company. Instead it's important to think of cybersecurity as a process that begins with a risk assessment of your

company: what would attract hackers the most and where are you most vulnerable? Once a risk assessment is complete, your company can develop a policy to improve your data security based on needs and budget.

Elements of effective cybersecurity include:

- Firewalls and Systems Rules
- Software Subscriptions
- Human Expert / Experienced Analysis
    - Malicious software reverse engineering support
    - Host, Network and Log Forensics
    - Rules testing and development
- Timely and Comprehensive Open Source Intelligence/Threat Intelligence
- Dynamic Security Capability

Constant Vigilance — Think of Cybersecurity as a Continuing Process to Protect Your Company!

- Risk Assessment
- Policy Development/Alignment
- Systems Engineering/Design
- Implementation
- Monitoring & Compliance
- Ongoing Oversight and Reassessment

Firewall and System Rules – this initial layer of cybersecurity protects companies the vast majority of threats. Sounds pretty good, right? Problem is this entry-point protection cannot stop targeted attacks, such as advanced persistent threats (APT).

Software Subscriptions – typical of what you see on your PC (such as Norton and MacAfee) these subscriptions can help clean up known viruses. They do detect new and unknown attacks. It's a reactive measure in which updates are not made until after a threat is discovered.

Human Analytical Efforts – this is arguably the most vital security element that many, supposedly, cutting-edge cyber firms do not address. It's important to remember that hackers are human adversaries who at times are unpredictable who in a large part prey on social engineering the unsuspecting system user and you need to instill your own human analytic element. As much as cybersecurity depends on technology, it depends even more on people.

Dynamic Security Capability— when it comes to cybersecurity, you're only as strong as your weakest link. An effective cyber posture requires a disciplined risk-based approach to balancing investment and effort in combating cyber threats. One size does not fit all!

Training and Surveillance – People with permission to be on your network are a far greater threat to information security than outsiders. Human efforts entail training, monitoring sensors, noticing behaviors and making changes to address threats.

Cybersecurity Experts in Orchestrating All 5 Disciplines

Harmony Technology Services and **Active Canopy** have formed a powerful partnership that combines expertise in cyber technology and cyber services. Together they provide a layered approach with timely assessments so companies can be better prepared to address cyber threats instead of react to them.

Here's how they work together to protect companies like yours!

Harmony Technology Services

Harmony Technology Services works with clients in a number of ways to optimize performance of people, processes and technology while also helping to identify and mitigate dangers in the following ways:

- **Risk Assessment** – working with you to determine your specific data risks
- **Policy Development** – helping you define guiding principles to protect your company including network access policies and specific software protection requirements
- **Architectural Definition and Deployment** – determining your policy and needs to technical support (hardware and software) needed
- **Monitoring and Compliance** – to ensure that your policies are being applied and respond effectively to changing technical environments and threats

Harmony Technology Services has high-level expertise in the Department of Defense (DOD) space and proponents NIST framework for cybersecurity. They provide their clients with guidance in translating the NIST cyber framework into a business context without it becoming overwhelming. Likewise, they deliver continuing analysis and ongoing threat mitigation. Harmony Technology Services partners with clients for long-term cybersecurity partnerships from A to Z, with phased approach that includes:

  - Risk Assessment
  - Systems Engineering/Design
  - Implementation
  - Ongoing Oversight and Reassessment

Active Canopy

Active Canopy provides defense in depth that provides data security against cyber-attacks as their clients conduct their daily business. They help manage your networks and prevent data losses across a range of enterprise network and cloud environments and endpoints that include servers, workstations, gateways, exchange servers and storage devices including:

- An excellent packaging of cybersecurity services for different levels of protection
- Flexible packaging of cybersecurity services to meet customers unique requirements
- A secure cloud you can trust
- The latest cyber threat intelligence that includes both open and closed sources of data
- Network, endpoint and log forensic collection and analysis
- Big Data – Data Science approach to finding bad behavior security events

Active Canopy fields an Active Defense for its clients. It starts with the analyses of gathered information from open and closed sources and a network of cyber security professionals. They then marry that information up with intelligence gathered from real-world hack attempts on their clients and external attempts, capturing, assessing and addressing those attacks – while at the same time better informing all of Active Canopy's clients about potential threats.

In doing so Active Canopy actively remediates host compromises and can isolate the host from the rest of the network to mitigate threats. They also use threat intelligence for situational awareness to better understand customer risks in order to recognize the context of their threats and attacks. All of this means that Active Canopy clients benefit from their expert capability at an affordable price. The best part is that all of this is done with a "light footprint", meaning that they provide flexible service meant to change with the customer's enterprise landscape, eliminating any technology "lock-in".

National Institute of Standards and Technology
U.S. Department of Commerce

The NIST Cybersecurity Framework

Developed by the National Institute of Standards and Technology, the NIST Cybersecurity Framework is a compendium of best practices and security standards that is accepted by the White House, governmental agencies and many corporate institutions as the Federal Standard for cybersecurity. This framework needs to be understood by organizations before a breach happens, because once it does and a response is conducted by federal law enforcement investigators, the initial questions will include if NIST Cybersecurity framework was being implemented.

NIST parameters represent a compliance-oriented approach and emphasize and encourage a proactive risk-management that builds on standards and compliance. Industries should adopt the guidelines as a key tool to manage and mitigate cyber risk to their business, in combination with other cybersecurity processes.

- **Identify:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities
- **Protect:** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services
- **Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event
- **Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event
- **Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event

The Bottom Line

Remember, your level of cybersecurity depends on three factors: the risk you are willing to take, the robustness of the system in place, and the costs you are prepared to pay. By partnering with Harmony Technology Services and Active Canopy you will help minimize the impact of threats to your company's data while protecting your business continuity, customer confidence, business investments and opportunities now and in the future.

Everyone now needs cybersecurity as sensitive data is stored globally and your network boundaries become less clear. You need peace of mind to know you are protected as best as possible and cost effective to your means. You need cybersecurity to be as flexible as your needs and at an adaptive pace that rivals today's threats. Harmony Technology Services and Active Canopy are your answers.

For more information about how your company can reduce the risks of hackers, contact Harmony Technology Services at (703) 546-4949 or via email at info@harmonytechnologyservices.com.