*Best Practices in Computer Network Defense: Incident Detection and Response*
*M.E. Hathaway (Ed.)*
*IOS Press, 2014*

*doi:10.3233/978-1-61499-372-8-30*

# Advanced Technologies/Tactics Techniques, Procedures: Closing the Attack Window, and Thresholds for Reporting and Containment

JOHN N. STEWART
*Cisco Systems and*
*Council of Experts, Global Cyber Security Center (GCSEC)*

**Abstract.** New techniques, tactics, and procedures (TTPs) are now available to strengthen security postures and become more resilient to cyber threats. Most of these technologies are accessible and affordable, and they are showing promising results. This paper exemplifies eight specific advanced techniques, tactics, and procedures to counter cyber threats, including using moving target architectures to confuse the adversary, monitoring the dark space of the Internet, and using honey pots to detect adversaries and infected machines within an organization's infrastructure. It also explains what is required to enable these techniques and what metrics should be used to measure their results. These advanced practices should become common security standards.

**Keywords.** Advanced persistent threat, cyber attack, cyber security, dark space, data exfiltration, domain name service, honey things, honey tokens, identity, indicators of compromise, metrics, misinformation, moving target, patching, reconnaissance.

## Introduction

Internet-connected devices have proliferated to such an extent that in 2008 more connected devices existed on Earth than people. The trajectory continues; some reports projecting that by 2020 the number of devices connected to the Internet will exceed 50 billion.[1] Cars are coming online, homes are automated with Internet Protocol (IP) based technology, hospital operating rooms have wireless networks, saltwater treatment plants are configuring IP addresses on the boilers for remote control and system feedback, and military systems are using connectivity and information as the warfighter edge.

The rapid spread of Internet-connected devices carries its attendant risk: a new piece of malware is detected every 2.2 seconds.[2] The number of breaches in the past twelve months exceeded 850, with 174 million records compromised.[3] A well-known DDoS campaign against various US banks has been ongoing for over a year. In two other examples, one company had 30,000 computers infected[4] and rendered inoperable via a directed attack, and a few others had the Advanced Persistent Threat 1 (APT1) hacking team active in their network for over four years, and all the while over 85% of breaches took at least one week to detect.[5]

The effects of such attacks are immediate and tangible: intellectual property (IP) and personal information stolen; services disrupted; systems erased; and networks compromised. Sophisticated hacking teams are very active and can operate entirely undetected for long periods of time.

It is equally instructive to note how dependent we are on technology for our day-to-day lives, including civilian and military operations. The mobile phone is the primary means of communication. Information availability is now the sought-after military and business operational edge against adversaries and competitors respectively. Our economy is now tied to this technology evolution: countries' GDP growth is directly affected by high ICT, be it when 10% of the population is connected, the GDP goes up 1-2%, or how digitization provided US$193 billion to the world economy in 2011.[6]

All told, we no longer use IT systems – we rely upon them.

The increase of connected devices and online services creates an expanded attack surface for would-be attackers. In other words, we now have a situation ripe for attacking combined with a robust population of adversaries who are increasingly motivated, trained, and confident. Given all this, we need to ask ourselves: 'What can be done now that tips the scales back in our favor, what does it take to get there, and how can I measure my progress?'

Included in this paper are eight advanced techniques, tactics, and procedures (TTPs) for meeting our needs head on, what is required to enable them, and five quantitative metrics to measure progress.

## 1. Advanced Tactics, Techniques, and Procedures

The security domain is an ever-evolving discipline where measure and countermeasure are developed in turn, and where new ideas emerge in all organizational verticals. New, emerging techniques are always coming to the fore. Twenty Chief Information Security Officers (CISOs) and security operators,[7] whose work protects companies worth over US$500 million in combined market cap, were interviewed for this paper. Their experiences and cutting-edge practice highlight three areas that reduce attack surface, lower the adversarial opportunity, and tip the scales in the defense's favor. These three areas are:

- Basics must be mastered:
  - Patching
  - Identity: Strong Identity, Federated Identity, and Identity Based Networking
  - Eliminate Dark Space
- Create doubt in the adversaries mind:
  - Moving Target
  - HoneyThings / HoneyTokens
  - Misinformation
- Analyze data and traffic for Indicators of Compromise (IOCs):
  - Local Data *Analytics*
  - Global Grids: The Eye in the Sky
  - Analysis of non-conformant protocol traffic, local or global

## 2. Basics Must be Mastered

We often believe that the latest technology will solve our problems, losing sight of what we can actually control—our own infrastructure. Do not be fooled by the seeming simplicity, because mastering the basics is actually an advanced approach. While the security industry continues to innovate, seeking another appliance, another software module, and another 'best practice', the fundamentals tend to remain the same. No matter how many modules and best practices exists, there are three elements to a successful attack: means, motive, and opportunity. Since an adversary's means and motive are generally beyond our control, we must focus on the one thing that is always within our control: opportunity.

### *2.1. Patching*

Enterprise data rarely exists on certain metrics (patched systems, security architecture, vulnerabilities), but consumer data does. This is instructive for even the most hardened critics who argue that the two do not compare naturally. The average online citizen in Germany, for example, has 75 programs from 25 different vendors. Of these, 14% are using operating systems that are not fully patched, and another 7+% of the applications installed are also not fully patched.[8]

Even if, by comparison standards, we reduce this down to 1% for enterprises, there can be no doubt that the risk surface remains significant. That said, the risk exposure is higher, with 10% of enterprise company respondents indicating they have done a full job of implementing the basics, represented here as the SANS 'Twenty Critical Security Controls for Effective Cyber Defense.'[9] Implemented correctly, basics such as patching can begin to move the needle on the 'opportunity' scale, systematically reducing the attack surface which adversaries may breach.

Using formal methods, patches have an ability to reduce attack surface up to 67-70% just by application.[10] Patching has shown statistical evidence proving to reduce the attack surface, and yet the statistics also suggest that use of this effective method is inconsistent at best.

Note that patching is not just about servers and applications; it is also about the network – the fabric used to connect everything else. Using interview responses and experiential data, one can conclude that network maintenance, patching, auditing, and controls validation are areas lacking investment. Interestingly, with the network being the transport means for all other systems that connect, it would seem that this attack surface should be minimized due to its criticality.

### *2.2. Identity: Strong Identity, Federated Identity, and Identity Based Networking*

A less obvious basic that must be mastered is identity. There are three parts to this: strong identity, federated identity, and identity based networking.

Statistically, most users do not use or are not required to use a strong digital identity and password. Two-factor and one-time password authentication should be universally deployed on critical systems, if only to avoid the simplest of exploits: co-opting the actual password from a user or administrator to gain unauthorized access to systems. The probability of such a breach can be reduced significantly with two-factor and one-time password authentication. The end result of such authentication procedures

is that core infrastructure takes more time and effort to successfully penetrate, a clear goal for all of us.

In addition, federated identity—in which a user's credentials can be used again without creating another account—makes for a user-friendly experience, reduces the total number of accounts, and simplifies forensics after an incident. This is not Single-Sign-On (SSO) exclusively, however, as the identity federation can often be between multiple identity brokers. The end goal here is to simplify the user experience while simultaneously increasing overall difficult for an adversary.

The last piece is a more advanced use for identity—identity based networking. In this area, a user's identity, coupled with a variety of factors such as the system they are using, time of day, and location, all play a role in what the user can do at any given moment. An example would be how a financial controller in a public company, upon login, will be able to see applications and services based on which system they are using (smartphone versus in-office computer), where they are currently located (the office or on the road), and what time of day they are aiming to use the service (3am versus 10am).

### *2.3. Eliminating Dark Space*

In addition to standard methods such as traffic analysis, non-protocol traffic, and HoneyThings/HoneyTokens, one must also find and eliminate dark space, e.g. the 'blind spots.' Dark space is loosely defined in the security world and often refers to looking at the 'inverse' of what you see, to infer what you might need to know about it.[11] A simple example is a network map, where you see all the devices in your network, yet what you really need to know is if there are network interfaces that are 'up' and you do not see the other side of the connection, or that you are running network devices that seemingly have no connectivity to the core network.

Dark space can hurt in the datacenter world too, because if scanners cannot analyze blocked data center segments then the risk analysis is incomplete for the data center. Finding and eliminating dark space, however, can be difficult because we are frequently taught to look at what *is* there, and rarely are we asked to look at what *is not* there and ask questions about it. That is precisely the line of questioning necessary to tackle this issue. The dark space will contain risks so becomes a natural attack surface for the patient, skilled, and/or lucky adversary.

### *2.4. Summary: Basics Must Be Mastered;*

Control what you can control, and do it well.

While things like patching, strong identity, or knowing your own infrastructure may seem obvious solutions rather than advanced techniques, leading practitioners are returning to the basics lower their risk through attack surface reduction. The reality is that while these solutions may sound like common sense, the activities mentioned—not investing in the latest malware detection versus fully investing in asset inventory and layer zero through seven services mapping,[12] deploying strong identity instead of fixed and complex passwords, and modeling and mapping the services your data center is providing—is actually quite rare. The 'basic' solutions turn out to reflect the most advanced thinking on the issue.

## 3. Create Doubt in the Adversaries' Mind

### *3.1. Moving Target*

One can make a rational argument that the reason data center systems are frequently and easily compromised is that they are relatively stationary. Data center systems do not 'change' much from one day to the next—the IP addresses, service, machine names, and configurations change infrequently—so an adversary may study them over time. Moving targets, on the other hand, create confusion for the adversary and create more difficult environments to maintain persistence in, and are now technologically possible. Two moving target examples are virtualization and Software Defined Networks (SDN).

Using virtualization and virtual machine clusters in data centers, you can reboot at will and/or randomly without interrupting service. This 'start from scratch' approach makes the virtual machine jettison malware if infected, as well as interrupting any covert, undiscovered activity from continuing onto the host. Lastly, virtual machines can reset the system baseline, which can potentially illuminate a re-infection attempt if instrumented to do so. A key element to success in virtualization is Intel Trusted eXecution Technology (TXT) or similar capability, which helps ensure the software and service validity. Additionally, control instantiation must reinstate from a clean slate as well (virtual firewall context, for example), which defines a baseline known-good, further allowing for compromise detection.

Software Defined Networks (SDNs) are a new approach that separates decision-making in the control and data planes. In the security realm, SDNs have rather unique applications. For example, you can now choose which traffic to send through your bandwidth/processing restricted security engines such as Data Loss Prevention (DLPs) systems, instead of sending all of your traffic through them. You can make this decision on-the-fly, adding an additional flexibility for you and additional confusion for your adversary.

In addition, you can dynamically segment your network, which makes the network appear as if it was reconfigured. Alternatively, during a successful attack, you can dynamically quarantine infrastructure and systems. You can also create a 'ghost network' to confuse the adversary, increasing their cost and risk.

### *3.2. HoneyThings/ HoneyTokens*

Honeypots are commonly used in networks to attract interest from adversaries, after which people study the adversary's techniques, slow them down, or ultimately defeat the adversary by detection. While HoneyThings and HoneyTokens are not new—the terms were coined nearly a decade ago—they are emerging as a sophisticated counter intelligence technique when used pervasively. Ghost machines in an infrastructure that have no real value, but look attractive; source code modules that essentially do nothing, and can be found in other products if IP is illegally copied; fake database accounts that are only interesting for malicious queries;[13] fake email addresses on mailing lists which will inform the owner if the list is copied; the list goes on.

The key here is baiting, where the value of the asset is not necessarily the asset itself, but rather the attraction and detection that result from another's interest in the asset. The end goal is detection, not prevention, and it may well be you can detect other machines infected or controlled within your own infrastructure or that you can affirm your IP was illegitimately re-used in another commercial product.

### *3.3. Misinformation*

While the tactic is controversial to some, misinformation offers another route to create adversarial confusion. Misinformation campaigns include a range of tools, including: monitoring the underground anonymously; introducing false information; allowing a hacker to continue to operate uninterrupted in order to learn their technique (making them believe they cannot be seen); and many others. The major risk of misinformation is that you end up confusing both the adversary and yourself. In order for this method to be effective, the misinformation must only disrupt the adversary, otherwise it is best to be prepared for unintended consequences. For example, if you falsely communicated that an attack was unsuccessful—doing so, of course, in an attempt to create doubt in the adversaries' mind—even though it clearly was, you may also find yourself violating other controls if the truth were to emerge.

### *3.4. Summary: Create Doubt in the Adversaries Mind;*

Shake the Confidence of our Adversaries.

In *the Art of War*, Sun Tzu wrote 'The whole secret lies in confusing the enemy, so that he cannot fathom our real intent.' In this case, our enemies are those attempting to illegally copy, disrupt, or destroy our information and systems, and one way to deter and defeat them is to confuse them using virtualization, HoneyThings, and even misinformation campaigns which can all lead them down a bridge to nowhere. In short, these tactics force adversaries to spend time and energy on path that are ultimately wrong, wasteful, and dangerous.

## 4. Analyze Data and Traffic for Indicators of Compromise (IOCs)

Too few organizations use the most powerful source they have: data. There are two complimentary methods for using data to disrupt attacks: local and global data analytics. Successful protection for your organization requires both.

### *4.1. Local Data Analytics*

Local data *collection* is a common practice, while local data *analytics* on that data is not common, except forensically. Analyzing protocol traffic to ensure it is allowed to go to and from authorized places is standard practice, while dropping malformed packets and alerting the SOC it happened is incredibly rare. There is opportunity to level up here.

For advanced local data analytics, two data sources emerge:

- Netflow/jflow/ IPFIX and Domain Name System (DNS) data;
- Netflow/jflow/cflow are record formats that indicate, among other things, the source and destination IP addresses and ports which two systems attempted and possibly succeeded in communicating upon. A rudimentary comparison to 'call records' in the phone world, network and security operations leverage this for seeing Advanced Persistent Threat (APT) malware callouts, for data

exfiltration successes and attempts, and deployed internally to a network, lateral movement for malware from machine to machine.

Domain name system (DNS) traffic capture and analysis provides insight into where computers are seeking to go, as a result of seeing what 'name' on the Internet is asked for, security and network operators can see if well known bad sites are asked about by systems (e.g. are users going to known malware sites), or if unusual DNS activity is requested to resolvers such as a reverse pointer record (PTR)[14] which goes nowhere.[15]

A key question that needs an answer is this: what is good, and what is bad? The answers vary from organization to organization, and in the end, will likely be stitched together with base lining actual traffic, and then loading up known bad IP addresses, domains, command and control (C&C) server IP addresses and black-hole routes, using the combined list to check the local data to see if there are IOCs.

### *4.2. Global Data Analytics, the Eye in the Sky*

Complementary to local data analysis is the subscription and connectivity to global data and threat analytic platforms. Anti-virus vendors, SPAM filters, and reputation analysis engines are online with sensors numbering in the thousands to millions. These global grids give each participant access to otherwise inaccessible data. In doing so, these systems provide machine level and human readable analysis which is more complete than any one of us could amass individually.

This connectivity can be machine based with web filters, BGP black-hole routes, email SPAM filters, and anti-virus, or can be human readable tailored threat reports, which provide a view from the outside to your network about IOCs.

### *4.3. Analysis of Non-conformant Protocol Traffic, Local or Global*

An unintended security technology side effect is that IOCs are often unseen due to the technology *doing what it was designed to do and not more*. In an ironic twist of fate, when traffic is dropped purposefully to protect against threat, that dropped traffic may well indicate a second problem needing solving solution: a compromised host.

For example, a web proxy can inspect port 80, 443, and other pre-defined web port traffic to ensure that malware-laden websites are not connected to, questionable content is filtered, and authorized sites are permitted. This same technology, however, will often silently drop traffic that does not appear to be web traffic – and it is in *that* traffic that an IOC hides. DNS servers do much the same, as do email gateways, yet in each and every case if the dropped traffic were analyzed for IOCs, you increase the chances for seeing infected systems.[16]

### *4.4. Summary: Analyze Data and Traffic for Indicators of Compromise:*

Use data to drive decisions, not emotion.

With local data analytics, 'your' world becomes clearer – which systems talk to one another, which are studied and attacked, which are vulnerable, which are resilient, and which are connected. Global data analytics connect the dots, so an attack campaign targeted at banks becomes clearer, as does a protocol attack against a specific

technology, which benefits us all. Studying non-conformant traffic in each shows how our adversaries try to hide using openings we authorized, just not for them.

## 5. Change the Mental Model

When it comes to security, changing one's *actions* is just as important as changing one's *thoughts*. For example, when you read a phrase like 'mastering the basics,' your gut reaction may be that such a thing is obvious—of course the basics should be mastered. The subtlety is that mastering the basics is not advanced *technologically*, it is advanced *intellectually*. Why? Today's security practices often lead us down a path to the latest technological tool or gadget, not realizing that 'good hygiene' (i.e., mastering the basics), likely lowers risk more.

### *5.1. Assume Compromise*

Unfortunately, the reality is that what was once surprising is now normal: networks and environments are penetrated regularly and many network teams are now assuming they have been successfully penetrated and use detection as the vehicle to discover it. This mental model is inherently conflicted – the defense is presumed to have failed. Assuming compromise is not giving up; protecting critical systems is essential no matter what. This mental shift is about enabling detection.

### *5.2. Outsourcing*

Another trend is the outsourcing of security to another organization, which carries both risk and reward. For example, if talent is not available to hire or the work cannot be managed internally, then outsourcing may be the difficult, and ultimately correct, choice. A lack of talent at your company may mean having someone else protect you. This is an intellectual leap, because security is core to the success of many organizations and to place that in other's hands can be difficult and uncomfortable.

### *5.3. Defeat the Adversary vs. Try and Stop them from Getting in all the Time*

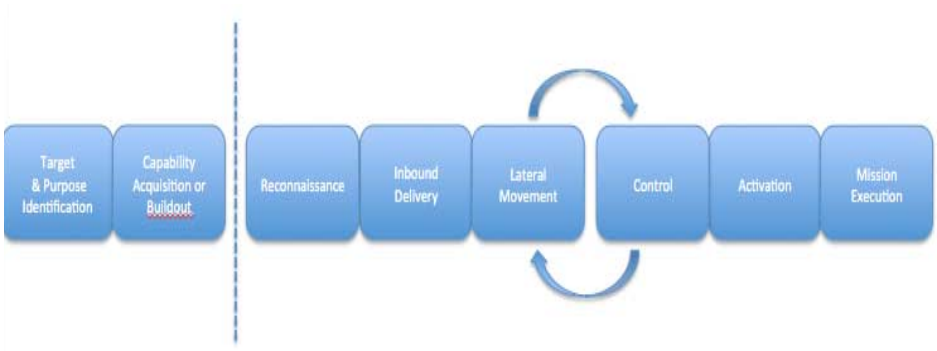


**Figure 1.** Cisco Systems Internal Kill Chain Model

A very subtle mental shift is to remember that stopping adversarial success is the most important goal, not necessarily stopping penetration or systems penetration per se. The

difficult thing to remember is that you can detect some things but not others, and that system infection does not equal operational failure *if the infection is not able to execute the mission*. This requires getting in the kill chain, to include detection of probes all the way to disruption in the final mission execution step.

### *5.4. Be Your Own Adversary – Hack Yourself*

Aggressively attacking your own infrastructure requires an intellectual leap: to best prepare yourself for anything, practice war gaming with live ammunition (exploits) on live targets (production systems).

Auditing your own infrastructure is a known practice for protection, although it has limited value as generally practiced today. Hacking (not auditing) yourself with your own team, however, has emerged as an entirely different, and possibly quite controversial, approach. The rationale behind the new method is that the hackers do not behave like auditors; they do not have predictable timeframes for their work, they break rules and laws, and they spend significant time in some cases before launching their attacks against critical infrastructure. So, the question is: why not behave just like they do?

To make the impact of a security threat real, it must personally affect an IT professional, a business executive, or a key developer. Acting like a true adversary (cognizant that the service you are attacking may go down, be corrupted, require costly repairs, etc.) is the new approach – you are acting just like the hacking community, and in doing so, preparing thoroughly. An unanswered question is: is hacking your own systems the right thing today to make it real?

### *5.5. Whitelisting*

It is ironic in the security world that we keep looking for the 'bad'—even though it is infinite—without focusing on known good, which is finite and achievable via whitelisting. Sometimes called the panacea for computer security, whitelisting is now practically applied as a noise reduction technique for both on-host, file whitelisting, for DNS domains for network flows, SPAM email gateways, and increasingly, for Cloud-based services. The underlying principle here is moving from 'blocking bad, and implicitly allowing everything else' to 'permitting good and denying everything else.' It can be said, unscientifically, that security's major practices are still in the first category.

Whitelisting takes multiple forms. On-host, it is all about legitimate files that do not need inspection since they remain whitelisted as good. For DNS, it is about dynamic domain filtering to determine good versus bad in a domain lookup. For traffic flows, it is topological knowledge about network configurations so that known traffic is permitted and all other traffic is implicitly denied.

The caution on these systems is remaining current, implying that knowing where to keep current on known good files, flows, domains is the essential component, and more often than not, not a core skill set for an organization to maintain themselves.

### *5.6. Summary: Change the Mental Model*

What got us here today will not carry us forward into the future.

Too often, common practice becomes correct practice, and in so doing, the needed changes are difficult to absorb, since we have trained ourselves to believe in the common. Mental model switches are essential in our industry right now because our mental models are holding us captive.

## 6. Progress Indicators and Thresholds: Metrics

You get what you measure, as management training asserts, and this field is no different. Yesterday's metrics were binary: breached or not. Today's metrics are combinatorial: breached or not, and the breach's impact. Tomorrow's metrics, which arguably some leading member states and companies are using now, are catalysts: adversarial dwell time, adversary confusion ratio, compromise speed, cost to protect vs. cost to lose or restore, and mitigation coverage percentage.

### *6.1. Adversarial Dwell Time* [17]

Measuring how long the adversary is inside your walls prior to you noticing is a lagging indicator that shows how effective your detection process is. Revisiting a common theme—opportunity—this particular metric helps gauge two things: how effective are you in seeing an adversary, and how long your adversary has to execute a mission. While the adversary may well be 'you' in this case (e.g. sponsored hack-a-thon activity), limiting time to detection and time for mission execution are the correct goals.

Dwell time can be safely detected by having red-team exercises, and these will both tell you how fast something is detected, and how fast the activity is disrupted. If not fast enough for both, the red-team mission may well succeed. Because you control both the attack and defense in these exercises, both will learn.

Forensics also provide insight into dwell time, namely research into a successful attack build, a timeline that sometimes goes all the way back to the reconnaissance.

### *6.2. Compromise Speed*

Consistent with adversarial dwell time is compromise speed. In measuring how long it takes various sophistication levels to compromise, disrupt or destroy a target, you learn if the target's protection and resiliency are up to the level expected. To measure effectively means to act like the adversary, either you or a provider. Red Team/Blue Team exercises are often designed with this goal in mind. These exercises are not fully effective as they otherwise could be, however, due to legal restrictions imposed on one of the teams (restrictions which your adversary will ignore). To be truly ready to face your opponent, then, you must think and be able to act like him.

There are multiple adversarial models to be considered. These include, but are not limited to:

- Having internal organizational knowledge;
- If the adversary completed some or significant reconnaissance;
- Was there insider assistance for the attack;

- Malware capabilities (to include at what level, ability to deploy, targeted not targeted);
- Value for the target.

In the end, the goal is to properly model whether your valuable assets, information or services can remain resilient long enough before the 'dwell time' timer for your organization, on average, expires and detection and countermeasures disrupt the attack.

### *6.3. Unmitigated Attack Duration*

It is accepted that attacks come in different forms, and if an attack is successful quickly, yet the effects are prolonged, then the attack itself is only halfway to measuring the overall duration. For example, if intellectual property is stolen via a compromised computer, the computer compromise is only one part of the attack's duration. Attack duration is the time from beginning to end of the kill chain (see Figure 1), and may not easily be measured, as you won't always know when *Target* and *Purpose Identification* happened.

That said, some attacks such as DDoS do have an ability to be measured for success from the beginning to the end, and the time in which the attack is effective becomes the metric to use. There are multiple ways to measure this mathematically, starting with the 'time the attack began until the time the mitigation abated the attack.' This may be augmented by using lost revenue or cost to mitigate (see below on mitigation vs attack costs), which aid in true cost through weighting. Why? Because the first five minutes of an attack may well be much more costly than the next fifteen minutes, even if the entire twenty minutes were before the mitigation. For example, if a financial trade must be completed by 1pm, the attack starts at 1255pm and lasts for twenty minutes, the first five minutes were the most costly – because the trade did not happen, and the mitigation didn't arrive fast enough.

### *6.4. Adversarial Confusion Ratio*

One of the elements that affect Compromise Speed and Dwell Time is adversary confusion, e.g. the delays injected into the mission and its goals due to confusion in the adversary's mind.

The adversarial confusion ratio is calculated in two pieces. Take the time confused divided by the total time, and take the number of incorrect decisions created by countermeasures versus the total made. Unless able to talk to your adversaries, which as strange as it might seem does happen from time to time, you will need to rely on Red Team/Blue Team exercises to know for sure.

Technological implementations already proven today include rebooting virtual servers randomly, and over short periods, to eliminate persistent command and control; using software defined networks to dynamically re-route traffic into a simulated environment, thus removing the conflict from the production environment; and using IPv6 enumerated networks to create a broad threat surface to have to hunt in, while simultaneously not using naming conventions for resources that make much sense (and are enumerable). In addition, using Software Defined Networks (SDN) is already proving useful to splice connections from original source to original destination and both increase visibility dynamically[18] (think lights going randomly on and off at night versus a prowler), and change the topological appearance to an adversary through traffic breaking and dynamic reroute.[19]

### *6.5. Cost to Protect vs. Cost for Losing/To Restore*

While never an ideal information security practitioner's answer, it is quite reasonable to look at what it will take to protect something versus its actual value, and its secondary value (both are important here). If the customer data is information that is not under legal or regulatory protection (primary), the cost of protecting it from illegal copying may outweigh the need. If the cost from the court of public opinion on breach is significant (secondary), then the secondary may outweigh the primary. Simply stated: if you are spending more to protect something than it is worth, why is that?

The balance is the essential piece here, and its and the balance is affected by risk tolerance, industry, capability and means.

### *6.6. Summary: Progress Indicators and Thresholds*

> Don't confuse hard work with results.[20]

Security efforts need clear progress indicators. In order to truly know what the results are, it is necessary to define the means used to measure them ahead of time, and then monitor them accordingly. Budget is not a success measure for security, nor is headcount, organizational structure, or title. Instead, how fast an adversary can exploit your vulnerability, for how long, and how much it might cost versus protecting become the litmus tests for our own progress.

## Recommendations and Conclusions

As an insight to what is working, and how well it is working, the TTPs and indicators provided here give a means to answer the questions: 'what can be done now that tips the scales back in our favor, what will it take to get there, and how can I measure my progress?'

With ICT having such profound effects on a nation's economic and security wellbeing, the question must be answered and it will be different for each country or service that asks it. It must still, however, be answered. Albert Einstein once observed that the definition of 'insanity' was to do the same thing over and over again expecting different results. Our industry can fall into that trap, and by some observables, we are in that trap right now. Our adversaries are more than happy to stack rank our defense teams, going after the weakest, using our practices against us. We cannot afford that outcome.

On a positive note, progress suggests that the advanced practices listed here will be standard soon enough, requiring a refresh or perhaps a brand new paper such as this. We owe it to ourselves to make these practices 'standard,' and to bring that day here faster.

## References

[1] Cisco, 2012. Cisco Connected World Technology Report. [online] Available at: <http://www.cisco.com/en/US/netsol/ns1120/index.html> [Accessed 30 October 2013].

[2] Dixon, J., 2008. The Risk of Operating in an Inter-Connected Society. [pdf] Team Cymru, Available at: <http://www.team-cymru.com/ReadingRoom/Whitepapers/2008/risk-interconnected-society.pdf> [Accessed 30 October 2013].
[3] Verizon, 2013. 2013 Data Breach Investigations Report. Available at: <http://www.verizonenterprise.com/DBIR/2013/> [Accessed 30 October 2013].
[4] Infosec Island, 2012. Saudi Aramco Investigation. Available at: <http://www.infosecisland.com/blogview/22290-Whos-Responsible-for-the-Saudi-Aramco-Network-Attack.html> [Accessed 30 October 2013].
[5] Ibid. 2013 Data Breach Investigations Report.
[6] World Economic Forum, 2013. The Global Information Technology Report 2013. [pdf] Available at: <http://reports.weforum.org/global-information-technology-report-2013/> [Accessed 30 October 2013].
[7] Interviewees that agreed to be referenced by name include : Malcolm Harkins, Intel; Roland Cloutier, ADP; Barry Hensley, SecureWorks; Christopher Fajardo, Blizzard Entertainment; and Phil Venables.
[8] Secunia, 2013. German Country Reports. [online] Available at: <http://secunia.com/resources/countryreports/> [Accessed 30 October 2013].
[9] SANS Institute, 2012. Twenty Critical Security Controls for Effective Cyber Defense, version 4.1. [online] Available at: <http://www.sans.org/critical-security-controls> [Accessed 29 October 2013].
[10] Manadhata, P., 2008. An Attack Surface Metric. Ph. D. Carnegie Mellon University. Available at: <http://reports-archive.adm.cs.cmu.edu/anon/anon/usr/ftp/2008/CMU-CS-08-152.pdf> [Accessed 30 October 2013].
[11] Llod, M., 2013. Dark Space: What You Don't Know Can Hurt You. Security Week. [online] Available at: <http://www.securityweek.com/dark-space-what-you-don't-know-can-hurt-you> [Accessed 30 October 2013].
[12] Layers 0 through 7 refers to the Open Systems Interconnection (OSI) model, which connects the physical (layer 0) through the application layer (layer 7) in a network, with everything in between. Wikipedia contributors. 'OSI Model.' Wikipedia, The Free Encyclopedia. [online] Available at: <http://en.wikipedia.org/wiki/OSI_model> [Accessed 22 October 2013].
[13] Spitzner, L., 2010. Honeytokens: The Other Honeypot. Symantec [online]. Available at: <http://www.symantec.com/connect/articles/honeytokens-other-honeypot> [Accessed 31 October 2013].
[14] Wikipedia contributors. 'List of DNS Record Types.' Wikipedia, The Free Encyclopedia. [online] Available at: <http://en.wikipedia.org/wiki/PTR_Record#PTR> [Accessed 22 October 2013].
[15] Lima, S., 2013. DNS and Advanced Persistent Threats (APT). [online] Available at: <http://www.cloudshield.com/blog/dns-security-expert-series/dns-and-advanced-persistent-threats-apt/> [Accessed 31 October 2013].
Jerrim, J., 2013. Detecting Malware P2P Traffic Using Network Flow and DNS Analysis. Damballa Inc. [pdf] Available at: <http://www.cert.org/flocon/2013/presentations/jerrim-john-detecting-malware.pdf> [Accessed 31 October 2013].
[16] Villeneuve, N., and Bennet, J., 2012. Detecting APT Activity with Network Traffic Analysis. Trend Micro Incorporated [pdf] Available at: <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-detecting-apt-activity-with-network-traffic-analysis.pdf> [Accessed 31 October 2013].
[17] Author's note: one of the leaders in Dwell Time is Jeff Brown and other colleagues at Raytheon, who introduced me to a new way of looking at this particular metric.
Marra, S., Hassell, S., Eck, C., Moody, J., Martin, S., Ganga, G., Harvard, K., Rickard, E., Sandoval, J., and Brown, J., Cyber Resiliency Metrics for Discussion. Raytheon [pdf] Available at: <http://bbn.com/resources/pdf/whitepaper_CyberResiliencyMetricsMASTERv4.pdf> [Accessed 31 October 2013].
[18] Groves, R., and Benetti, B., 2013. Microsoft's Demon: Datacenter Scale Distributed Ethernet Monitoring Appliance. Microsoft [pdf] Available at: <http://sharkfest.wireshark.org/sharkfest.12/presentations/A-4_Leveraging_Openflow_to_create_a_Large_Scale_and_Cost_Effective_Packet_Capture_Network.pdf> [Accessed 31 October 2013].
[19] Heckman, K., 2013. Active Cyber Network Defense with Denial and Deception. [video] CERIAS Seminar: Purdue University. Available at: <http://www.cerias.purdue.edu/news_and_events/events/security_seminar/details/flash/6ptedmqa1kgtk3au4jmiplp0v8> [Accessed 31 October 2013].
[20] Fortune 50 CEO.