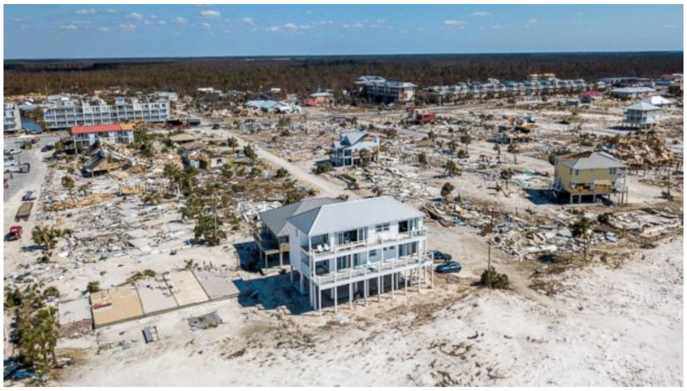
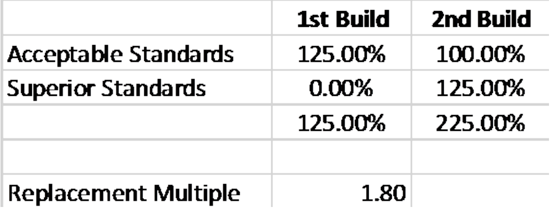
An Ounce of Prevention is Worth a Pound of Cure

(by David Daugherty and Scott Blackard)

In an age where we seem determined to experience the mistakes of our ancestors, conventional wisdom sometimes pops up in unexpected places. In 2018 we can find the value of conventional wisdom in preparation for inclimate weather. I was writing the DIYers article perched in the den, watching the devastating impacts of hurricane Florence on North Carolina. Two months later hurricane Michael flattened Mexico Beach in the Florida panhandle.

When it comes to conventional wisdom, mother nature can be a pretty good teacher. If you want to be prepared for inclimate weather, you need better construction standards. In the illustration to the right, the results of planning and preparation could not be clearer. In a neighborhood where everyone else built to current standards, the only home left standing is the one built using superior construction standards. In this case the builder spent roughly 25% more on construction than his neighbors and survived unscathed.





	1st Build	2nd Build
Acceptable Standards	125.00%	100.00%
Superior Standards	0.00%	125.00%
	125.00%	225.00%
Replacement Multiple	1.80	

Let’s do the math. If we assume that all those who lost their homes learned a lesson and spend an additional 25% to rebuild, their total build costs will be 180% of what it would have cost to use superior standards in the first place. Mother nature is indeed a good teacher.

In another event, even closer to my home in Texas, torrential rain washed out a bridge over the Llano river and took out a four lane, concrete bridge and the primary fiber link for five central Texas counties.

In this case an ounce of planning could have saved weeks of downtime for residents and millions in related costs to local businesses. Considerably more than a “pound of trouble”. In this case we can assume that the replacement multiple will be higher than 1.8.

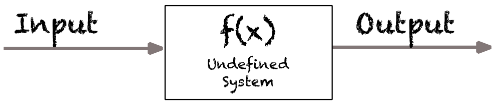
The internet, much like the weather is unpredictable. With potentially one notable exception. We KNOW that *future* demand on the internet will present unanticipated design and operational challenges. “So when it comes to internet, why are we using design and operating standards tuned to *today’s* needs?” Why not take a hint from mother nature and pay for an ounce of protection?

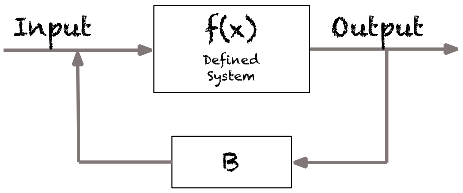
Business Stability

Unfortunately, standards are static and will only take you so far. Given increasing rate of change in technology and consumer demand, there must also be a dynamic component that continually monitors and adjusts performance necessary for temporal stability. In engineering terms this is called feedback.

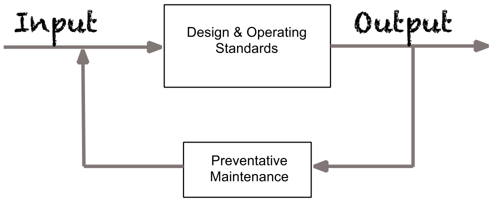
What makes this an even more complex problem is an equally rapid integration of the internet and business. The internet has become such an integral part of most businesses that design, and operating standards must evolve to include business operations. As it turns out, this may not be as intimidating as it sounds, if we approach this like any other engineering problem. In this case we will use lessons from Control Theory typically included in most college engineering curricula.

One of the first things that they teach you in control theory is the definition of a chaotic or unpredictable system. It goes something like this. The output of any system f(X) is unpredictable, undefined or chaotic without feedback (called beta - B).





This is a basic engineering principal that can be applied to how internet infrastructure is designed and operated. Beta is this case is active customer feedback used to maintain stability over time “temporal stability”. This may not like conventional wisdom, but it is. It is applied in business every day when merchants ask their customers for feedback. Regardless of format, this information is used to adjust products and services to meet market expectations.



From a business perspective, the design standard f(x) is your business plan. It spells out exactly how your business is designed and operated. It also provides guidance on how your business should perform over time. From a technical perspective design and operating standards dictate how your communications infrastructure is designed, deployed and operated to achieve business goals and objectives and spelled out in the business plan.

In mechanical systems, for example, preventative maintenance is used to make sure that system components are serviced or replaced before they fail and bring down the entire system. For internet service infrastructure “preventative maintenance” provides the same basic service. It is comprised of customer feedback through a combination of face-to-face meetings and social networking. This information is then used to “tweak” customer services and improve and/or upgrade infrastructure.

This is one of the major drivers for broadband DIYers. This kind of business/infrastructure integration is so tightly coupled with business performance that it has become mission critical and cannot be relegated to incumbent ISPs. The most likely outcome, over time, is the formation of partnerships with trusted service providers and specifically tuned to the needs of the business.

Cyber Security

OK, so we are smarter than the average bear and learn from mother nature, what kind of standards do we use and where can we find them? It turns out that one of the things our government *is* good for is planning for inclimate weather, at least as far as the internet is concerned. Given all the recent concern over international hacking it might surprise you to learn that the government is pretty well prepared. They have been gearing up for “future” cyber threats since 2014. This is apparently not true for state and local government.

The good news is that the internet is changing human commerce in new and unexpected ways. “Alexa, mute the TV” has become an hourly refrain for many telecommuters. Just one year ago most of us would ask, “Who the hell is Alexa and what is she doing in my house?” Even more alarming, advertisements have started coming in over subscription services like the Sonos music service, instructing Alexa to order things on my credit card. What’s next?

As internet-based services become a more complex, malware is undergoing a similar metamorphosis.

This is quite literally just the tip of the iceberg. The last image bait-click my wife made on a Pinterest, for example, activated embedded malware that quietly installed a trojan designed to record and transmit keystrokes to China! As internet-based services and human commerce become a more integrated and complex, malware is undergoing a similar metamorphosis.

A SOC is a facility that houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis.

CPE resident anti-virus software is a *passive paid subscription services are very active and typically coupled with the operating firewall.* This type of protection is not sufficient to address and eliminate the rapidly growing universe of cyber threats. The most likely solution to this problem must incorporate an *active* 24 x 7 live monitoring, complete with interdiction, remediation, services. This type of support operates in parallel with the Network Operating Center (or NOC) and is called a Security Operating Center (or SOC). From and operating perspective the addition of a SOC basically doubles the operating cost of the NOC. This has necessitated an industry retrospective on how internet services are packaged and priced. The requirement for active security services combined with the avalanche of new IoT technology is driving up operating costs and related contingent liability.

Our subject matter expert for this discussion is Clarus Broadband Chief Security & Information Officer Scott Blackard. Scott has been involved in several notable cyber projects over the last twenty years. This includes threat modeling for fortune 100 organizations, threat modeling and Cyber operations support for the US DoD/GOV, direct support to academia through Cyber Patriot and Collegiate Cyber Defense Competition, National Cyber League, Development of Training networks and curriculum to support the workforce. When not working Scott is an avid hunter and

fisher and combat sports athlete, he has 4 children in college and enjoys spending as much time with them as he can.

In recent years Scott has been involved with government organizations that have certainly not been in the public eye. “In 2014”, Blackard begins, “the Department of Defense (DoD) formed a cyber defense force known as Cyber Protection Team (CPT). Their mission is to provide mission assurance and threat mitigation support for US critical infrastructure.” CPT security services are provided in sequential layers and include the following: Identification, Protection, Detection, Response, and Recovery. These services have matured over the years and provide a solid foundation for the development and support of commercial and residential infrastructure.

Cyber Protection Team (CPT)

The National Institute of Standards and Technology (NIST) released version 1.0 of the Framework *for Improving Critical Infrastructure Cybersecurity*[1] on February 14, 2014. The Framework contains a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. It presents industry standards, guidelines, and practices. The Framework consists of five concurrent and continuous functions including Identification, Protection, Detection, Response, and Recovery.

Most currently available forms of cyber protection fall within Identification and Protection. In much the same fashion that the help desk uses “run books”, passive forms of cyber protection use white lists, black lists to Identify, protect and respond to known forms of malware. The SOC also uses “run books” and knowledgeable “security service personnel” to help Respond and Recover for new and ongoing security threats. “One of the more insidious characteristics of evolving cyber threats”, Blackard notes, “is that cyber threat also includes real time attacks from bad actors. These attacks employ the orchestrated application of both passive, active malware and real-time hacking to break into your network.” The only way to protect networks from this kind of attack is with the use of good actors known as “white hackers” and “counter hacking”.

White hackers and defense perimeter network administrators work as a team to control the security domain in a cost-effective manner for each network defended. “Offensive measures, or “strike back” or “counter hacking” activities”, notes Blackard, “are only relevant as a function of Automated Indicator Sharing (AIS). Counter hacking only occurs within specific parameters and boundaries agreed upon and approved by the Designated Approval Authority (DAA) to maintain the integrity of evidence or artifacts used to enhance ongoing operations”.

[1] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Automated Indicator Sharing (AIS)

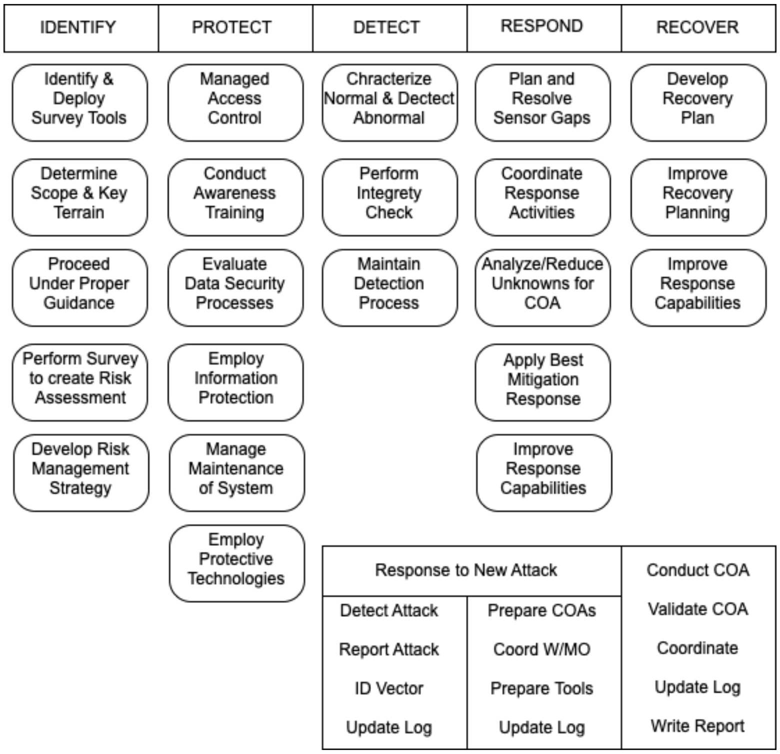
The Department of Homeland Security’s (DHS) free Automated Indicator Sharing (AIS) capability enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed. Threat indicators are pieces of information like malicious IP addresses or the sender address of a phishing email (although they can also be much more complicated).

AIS is a part of the Department’s effort to create an ecosystem where as soon as a company or federal agency observes an attempted compromise, the indicator will be shared in real time with all of our partners, protecting them from that particular threat. That means adversaries can only use an attack once, which increases their costs and ultimately reduces the prevalence of cyber-attacks. While AIS won’t eliminate sophisticated cyber threats, it will allow companies and federal agencies to concentrate more on them by clearing away less sophisticated attacks.

Ultimately, the goal is to commoditize cyber threat indicators through AIS so that tactical indicators are shared broadly among the public and private sector, enabling everyone to be better protected against cyber-attacks.

Source: https://www.us-cert.gov/ais

Over the years, CPTs have developed an operational matrix of sorts depicted below. This matrix is a basic list of activities in each of the five functions of Cyber protection.



IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Identify & Deploy Survey Tools	Managed Access Control	Chracterize Normal & Dectect Abnormal	Plan and Resolve Sensor Gaps	Develop Recovery Plan
Determine Scope & Key Terrain	Conduct Awareness Training	Perform Integrety Check	Coordinate Response Activities	Improve Recovery Planning
Proceed Under Proper Guidance	Evaluate Data Security Processes	Maintain Detection Process	Analyze/Reduce Unknowns for COA	Improve Response Capabilities
Perform Survey to create Risk Assessment	Employ Information Protection		Apply Best Mitigation Response	
Develop Risk Management Strategy	Manage Maintenance of System		Improve Response Capabilities	
	Employ Protective Technologies			

Response to New Attack		Conduct COA
Detect Attack	Prepare COAs	Validate COA
Report Attack	Coord W/MO	Coordinate
ID Vector	Prepare Tools	Update Log
Update Log	Update Log	Write Report

Mission Essential Tasks of A Cyber Protection Team

Identify

The first phase of protection is the identification of known, common cyber vulnerabilities. This information is typically updated and provided through third party virus protection software. These lists are provided through some kind of subscription services and are kept updated by cyber specialists for new threats. Hopefully before new vulnerabilities are tripped by unsuspecting subscribers.

Protection

Hardening an enterprise infrastructure is a large and time-consuming task, that typically takes a week or two. For vulnerable networks hardening steps should be taken in a deliberately prioritized order to ensure the threats can be detected, isolated and mitigated. All steps in the hardening process are important but the order they are executed is critical. During the hardening process the infrastructure can typically be defended if the attack can be detected. This makes detection the first and most important element of Protection.

Detection

The most important element of Detection is the ability to characterize normal and abnormal users, devices, software, and configurations. Everything must be analyzed as “known good”, “known bad”, or “unknown”. Unknown threats must also fit into one of two categories.

- Good is defined as authorized **AND** correct
- Bad is defined as unauthorized **OR** incorrect

Response

Now that we have detected a new and unknown cyber threat, damage is occurring. Every minute that the threat goes unaddressed, the cost of recovery increases. Damages will include the time required for cyber operatives to terminate the attack, assess and correct the damage. It also includes the costs of implementing security provisions designed to prevent similar attacks in the future.

Recovery

If we have reached the Recovery stage of protection, we have identified and terminated some form of previously unknown cyber threat. During Recovery Cyber security operatives restore normal network operations and fully document the new threat. This information is also used to update passive forms of Cyber protection.

Summary

If maintaining reliable internet access was not already sufficiently difficult, rapidly maturing cyber threats have added a whole new and expensive dimension to customer support. The good news is that the vast majority (99 %) of cyber threats are quickly and quietly dealt with through passive support systems. The bad news is that last 1% easily accounts for 99% of the cost and related damage of modern network operations. It is no longer a matter of ***if*** you will suffer a cyber-attack, it is a matter of how much it will cost you to identify, terminate and recover ***when*** you suffer an attack.