Strike a Blow for Freedom: Privacy, Security, Civility... Chaos

The core of the apple is rotten

Don O'Neill
Independent Consultant
Former President (2005-2008), Center for National Software Studies

The FTC is announcing a new forum called PrivacyCon to bring together leading privacy and security researchers with policymakers to present and discuss their latest findings. PrivacyCon seeks to expand collaboration among whitehat researchers, academics, industry representatives, consumer advocates, and regulators to address the privacy and security implications of emerging technologies.

Outline

- Opening
- Executive Summary
- Software 2015 *Situation Dire*
- Technical Debt: *Sources, Triggers, and Analytics*
- Privacy, Security, Civility... o Chaos
- Data Encryption: *At the Intersection of Privacy and Security*
- Free Riders: *Benefits and Pitfalls*
- Shifting the Paradigm of Cyber Security Blame: *From Supplier to Consumer*
- Privacy and False Claims: *False Light and Actual Malice*
- Cyber Security: *Fines and Cyber Insurance*
- Clean Room Software Engineering
- Next Generation Software Engineering
- Conclusion

Key Words

software situation dire, Technical Debt, Cyber attacks, privacy, security, data encryption, free riders, information sharing, false claims, fines, Cyber insurance, trustworthiness, STEM, software assurance, Clean Room Software Engineering, Next Generation Software Engineering

Opening

Cyber attacks represent a clear and present danger and a threat to the competitiveness and security of the nation. Yet our Cyber Strategy has been primarily driven by politics. Just consider the stresses surrounding privacy and security where privacy is the freedom and ability to reveal oneself selectively and security i the condition of being protected against danger o loss, both reasonable goal bu o collisio course nevertheless.

Is it possible to have both privacy and security? If not, then which are we entitled to... no matter what? Where civility is defined as the sacrifices we make for others, perhaps an appeal to civility would prompt people to agree to sacrifice some level of privacy in order to promote a higher level of security for others.

Whereas Cyber Security is reasoned about in terms of trust in systems, the collision between privacy and security revolves around trust i people Just what is th cost of Cyber Security protection in terms of civil liberties?

Contested by the government, does data encryption serve as the gate keeper for both privacy and security? Should claims of assuring privacy or security on the Internet in the absence of data encryption be considered false claims on their face?

Is it possible to bring the rights, values, and interests of the individual, business, and government with respect to privacy and security into a sustained equilibrium? Is it possible to reconcile dwindling government bargaining power with its presumed free rider role in the public commons?

Executive Summary

The increasing dependence of industry and government on an insecure Internet infrastructure built on an immature software profession whose promise exceeds its delivery has now become a source of risk that teeters at the tipping point. The convergence o software, national security, and global competitiveness interactions and their fragile dependencies are capable of unleashing a destructive synergy of propagating and cascading effects impacting privacy and security. The core of this apple i rotten.

Technical Debt is the organizational, project, or engineering neglect of known good practice that can result in persistent public, user, customer, staff, reputation, or financial cost. Technical Debt stems from ignorance, neglect, and even the intentional deferment of effort. Th neglect for which the project and enterprise will pay consequences in terms of interest on the debt includes systems and software engineering and management, systems and systems of systems, iterative life cycle model dynamics, and dynamic analysis and finite word effects. So clearly the scope of Technical Debt must be elevated and de-leveraged in order to trim privacy and security risk.

Cyber attacks represent a clear and present danger and a threat to the competitiveness and security of the nation. Yet our Cyber Strategy has been primarily driven by politics. Just consider the stresses surrounding privacy and security where privacy is the freedom and ability to reveal oneself selectively and security i the condition of being protected against danger o loss, both reasonable goal bu o collisio course nevertheless.

Data encryption, contested by government and slow to be adopted by industry, lies at the intersection o privacy and security. Basically plaintext is information that is input to a coding process, cleartext is information that is immediately understandable to a human being without additional processing, and ciphertext is the output o a encryption process featuring an algorithm that makes plaintext information unreadable to anyone except those who possess a unique key. To combat crime and terrorism, the government wants access to these unique encryption keys in order to return ciphertext to cleartext and its readable plaintext form; industry and its consumers and users objec to any sharing of encryption keys o privacy and security grounds.

Corporate board members, C-suite occupants, and government executives claiming ignorance of Cyber Security risks, threats, and challenges continue to operate as free riders in the Cyber domain. These leaders seem to take pride in not understanding the technology they depend on. This ignorance and neglect are often coupled with the stigmatization of the Cyber, software, and technology experts who know things that corporate board members, C-suite occupants, and government executives can never know without a STEM background now beyond their grasp.

The Internet was established to disseminate data and information. The Internet is not equipped to control, secure, or protect the data and information being disseminated. In actual fact the data and information that is transferred about on the Internet is not under control, is not secure, and is not protected beyond th due diligence associated wit backup and recovery operations. Responsibility for controlling, securing, and protecting the dissemination of data and information must lie with those who choose to entrust proprietary data and information to the Internet.

The result of a shifting definition of privacy and immature privacy practices, an uncontrolled Internet infrastructure and unproven Cyber Security practices, and free riders i free spirited Internet culture has led to frivolous privacy policy assertions, promises, and commitments that border on false claims. The unproven state of Cyber Security protection is well known by the experts in the field and less known and accepted by industry executives. An enterprise whose privacy policy commitments are not matched by a capability to meet the commitments made is presenting itself in a false light and where done knowingly is guilty of actual malice.

Th use o stiff fine for organizations who attract and suffer Cyber attacks through their lack of readiness, especially the failure to adopt a Cyber Risk Management culture, is both necessary and useful.

- *Necessary* because these organizations wit their unattended weaknesses and vulnerabilities actually serve as an attraction, even a magnet, for bad actors making everyone less safe.
- *Useful* because the permissive and voluntary alternative of Cyber Insurance with premium rates calibrated to Cyber readiness and Cyber Risk Management cultural maturity is in a state of failure to launch with entrenched resistance to sharing Cyber incidents and cost data pending indemnification or at least targeted liability. The Safety Act flirts with indemnification so long as a incident is declared a ac of terror. I too is in a state of failure to launch.

The uncertainties associated with a useful and credible Cyber Insurance market are wide ranging and depend on Cyber Security theory and foundations, reduction of theory to practice, the collection and use of empirical practice data, the validation of actual practices against the theory based on empirical data, information sharing, realistic premium setting, informed and trustworthy coverage, and straightforward dollar convertible Cyber consequences. These uncertainties have not yet been reduced to calculated risks. To what extent can Cyber Insurance also become punitive? Just as flood insurance may be denied to those who wish to build on flood plains, perhaps Cyber Insurance may be denied to the unprepared organization wishing to use the Internet for data and information it cannot afford to lose. So both fines and insurance can come with a punitive edge, and each can serve as carrot or as stick.

Trustworthiness requires a commitment to rigor in both software production and its verification. Software Assurance demands two capabilities associated with trustworthiness, the capability to produce trustworthy software products and th capabilit to verify tha software products are trustworthy. Each depends on engineering and technology rigorously applied. There is the need for a rigorously defined Clean Room method and process to produce a provably correct Clean System: one whose method possesses the means to investigate legitimacy, confirm intent and wherewithal of people, verify process execution, and validate outcomes achieved in determining that a legitimate Clean Room was in place and operation and one whose outcome is based on trusted software engineering principles and practices in producing provably correct software components.

In accordance with the austerity of the times, the immediate goal of practical Next Generation Software Engineering is to drive systems and software engineering to do *more with less... fast.* Four practical objectives are identified to advance this goal using smart, trusted technologies:

1. Drive user domain awareness;
2. Simplify and produce systems and software using a shortened development life cycle;
3. Compose and field trustworthy applications and systems from parts;
4. Compose and operate resilient systems of systems from systems.

Software 2015: *Situation Dire*

The increasing dependence of industry and government on an immature software profession whose promise exceeds its delivery has now become a source of risk that teeters at the tipping point. The convergence of software, national security, and global competitiveness interactions and their fragile dependencies are capable o unleashing a destructive synergy o propagating and cascading effects impacting privacy and security. The core of this apple is rotten. All this, while both industry and government continue to play the role of free rider as users of software lacking both the technical ability and political will to act.

The Software 2015 Report observed that software is the critical infrastructure within the critical infrastructure. This was the theme of the 2nd National Software Summit (NSS2 2005) Th 2015 Software Vision was then stated as *"Achieving the ability to routinely develop trustworthy software*

products and systems, while ensuring the continued competitiveness of the U.S. Software industry". Th question today is *Where do we stand with respect to the National Software Strategy and its programs?* Th answer, th situation is dire.

Recognize that competitiveness is like flood water finding or creating its own path. Competitiveness impacts both software and security as it favors offshore outsourcing and further impacts security as innovation drives towards mobile and BYOD. Recognize also that software and security are connected at the hip through the elusive attribute of trustworthiness and together impact competitiveness in a not so virtuous cycle (Defense AT&L, 2015).

Outcomes
In terms of National Software Strategy (NSS2 2005) outcomes, the situation is dire:

1. The increasing dependence of industry and government on an immature software profession whose promise exceeds its delivery has now become a source of risk that teeters a the tipping point.
2. The convergence of software, national security, and global competitiveness interactions and their fragile dependencies are capable of unleashing destructive synergy of propagating and cascading effects.
3. All this, while both industry and government continue to play the role of free rider as users of software lacking both the technical ability and political will to act.

Top Ten Reasons

1. Industry and government continue to increase dependence on software produced by an immature profession that has stumbled in delivering trustworthy software components, systems, and systems of systems to the nation's critical infrastructure and defense industrial base.
2. Th result i Cyber Security weaknesses and vulnerabilities seede by our best and brightest that are being exploited at will by persistent adversaries whose capabilities and motivation can only be guesse at by assessing the trace o consequence they inflict.
3. Essential Cyber Security foundations are lacking and so Cyber Security practice is ad hoc not well understood, and ineffective.
4. Premature Cyber Security training and certification programs do not yield the capability to secure large scale software intensive systems, research programs are misdirected, STEM initiatives promise what they cannot deliver, and executives and senior managers are disconnected from the realities they face.
5. Citizen concerns about privacy, civil liberties, and liability serve as obstacles to deter effective information sharing erecting barriers to achieving Cyber Security.
6. The increasing dependence on software to boost productivity and achieve competitiveness is not being met with increasing domestic workforce capability and capacity.
7. Instead, enterprises i search of value continu to choose offshore outsourcing for skills and cheap labor despite vigorous attempts to stigmatize this practice by politicians.
8. Cyber Security shortfall threatens competitiveness by easy and continuing loss of intellectual capital to nation states who drive on an information highway without rules or consequences.
9. Government tax policy, misguided regulations, and antitrust litigation offer additional impediments and uncertainty.
10. Underlying al this, th nation's austerity and affordability challeng has the effect of tyin our hands just when the starter's gun signals the start of the race for the twenty-first century. On top of all this, the will to act i lacking as the nation find itself i a leadership crisi (Defense AT&L, 2012).

NSS2 (2005) Software 2015: A National Software Strategy to Ensure U.S. Security and Competitiveness," Center for National Software Studies, May 2005

Defense AT&L (2015) O'Neill, D., *"Software 2015: Situation Dire"*, Defense Advanced Technology and Logistics (DAT&L) Magazine, May-June 2015
http://www.dau.mil/publications/DefenseATL/DATLFiles/May-Jun2015/O'Neill.pdf

Defense AT&L (2012 O'Neill, D., *"A Disruptive Game Changer to Achieve DOD Austerity",* Defense Advanced Technology and Logistics (DAT&L) Magazine, May-June 2012
http://www.dau.mil/pubscats/ATL%20Docs/May_Jun_2012/O%27Neill.pdf

Technical Debt in the Large:

The scope of Technical Debt from the viewpoint of the programmer is one of software components, cod an test activities, an static analysis. However, the neglect for which the project and enterprise will pay consequences in terms of interest on the debt includes systems and software engineering and management, systems and systems of systems, iterative life cycle model dynamics, and dynamic analysis and finite word effects. So clearly the scope of Technical Debt must be elevated and de-leveraged in order to trim privacy and security risk. (Defense AT&L 2013).

Technical Debt is the organizational, project, or engineering neglect of known good practice that can result in persistent public, user, customer, staff, reputation, or financial cost. Of course, Technical Debt stems from ignorance, neglect, and the intentional deferment of effort.
1 The ignorant d not know known goo software engineerin practice.
2. The neglectful may know known good software engineering practice but lack the respect and discipline to apply it rigorously as intended.
3 Those who intentionally defer work o take expedient shortcuts are arrogant practitioners who believe their superior skills will permit them to dodge the bullet of consequences for their action.

Technical Debt is an interesting metaphor. Its utility lies in its simplicity and ease with which complex software planning and technical issues can be framed for executives and managers who may lack the technical background to engage these issues firsthand. With this shorthand method of framing complex problems comes the loss of underlying detail that can restrict or misdirect the identification, analysis, and resolution of software planning and technical issues among those who do possess the technical background to engage these issues firsthand.

The success of large scale software intensive systems is largely dependent on the engineering, management, and process capabilities, people, practices, methods, and tools of the enterprise charged with the requirements determination, design, development, testing, fielding, and sustainment of systems and systems of systems. Within any organization, these elements of success are in various stages of maturity, and their evolution and alignment may become the source of strategic software management and continuous process improvement. At any point in time, these gaps can be referred to as Technical Debt when they result in persistent reputation, economic, mission, or competitiveness costs and risks. When these gaps are neglected, whether undiscovered or consciously ignored, Technical Debt may be incurred.

Technical Debt is considered written off only when it is eliminated. Draining the swamp depends on understanding and aligning the sources of Technical Debt in management, engineering, and process.

- Sources of Technical Debt in engineering involve neglect in application domain understanding, requirements determination, system and software architecture, iterative multi-level design, staged incremental development, software development life cycle, programming language, middleware, operating system, network interface, and software development environment.
- Sources of Technical Debt in management involve neglect in requirements management, estimating, planning, measurement, monitoring and controlling, risk management, process management, team innovation management, supply chain management, team building, personnel management, and customer relationship management.

- Sources o Technical Debt i process involve insufficien evidence of explicit goal an readiness to perform, insufficient accountability based on work responsibility matrix, insufficient planning of design levels and staged increments, and insufficient planning, management, and control of software product releases.

Defense AT&L (2013 O'Neill, D., *"Technical Debt in the Code: Cost to Software Planning",* Defense Advanced Technology and Logistics (DAT&L) Magazine, March-April 2013
http://www.dau.mil/pubscats/ATL%20Docs/Mar_Apr_2013/O%27Neill.pdf

Privacy, Security, Civility... or Chaos

Cyber attacks represent a clear and present danger and a threat to the competitiveness and security of the nation. Yet our Cyber Strategy has been primarily driven by politics. Just consider the stresses surrounding privacy and security where privacy is the freedom and ability to reveal oneself selectively and security i the condition of being protected against danger o loss, both reasonable goal bu o collisio course nevertheless.

1. Is it possible to have both privacy and security? If not, then which are we entitled to... no matter what? Where civility is defined as the sacrifices we make for others, perhaps an appeal to civility would prompt people to agree to sacrifice some level of privacy in order to promote a higher level of security for others.
2. Whereas Cyber Security is reasoned about in terms of trust in systems, the collision between privacy and security revolves around trust i people Just what is th cost of Cyber Security protection in terms of civil liberties?
3. Is i possible to bring the rights, values, and interests of th individual, business, and government with respect to privacy and security into a sustained equilibrium?
4. Is it possible to reconcile dwindling government bargaining power with its presumed free rider role in the public commons?

Data Encryption: *At the Intersection of Privacy and Security*

Data encryption, contested by government and slow to be adopted by industry, lies at the intersection of privacy and security. With data encryption an organization may achieve privacy and security assurance; without it, an organization i vulnerable.

Basically plaintext is information that is input to a coding process, cleartext is information that is immediately understandable to a human being without additional processing, and ciphertext i the output of an encryption process featuring an algorithm that makes plaintext information unreadable to anyone except those who possess uniqu key. This private encryption accords the most privacy and security assurance.

To combat crime and terrorism, the government wants access to these unique encryption keys in order to return ciphertext to cleartext and its readable plaintext form; industry and its consumers and users object to any sharing of encryption keys on privacy and security grounds. Encryption keys shared with the government is termed key escrow encryption. Encryption keys shared jointly with both the government and a vendor is termed split key encryption. Both key escrow and split key encryption reduce the level o privacy and security assurance. Table 1 evaluates th efficacy of four encryption techniques in terms of cost and benefit. The benefit being sought is full privacy and security assurance. The cost factors include degree of expertise needed, amount of effort required, and the degree of inconvenience imposed on users.

1. Th use o private encryption to fully achieve privacy and security assurance suggests that the adequate level of expertise and effort required are both low and that some level of inconvenience is imposed on users.
2. The use of key escrow encryption entails trust in government, thought to possess uncertainty, to achieve some level of assurance and suggests a medium level of expertise and effort and that some level of inconvenience is imposed on users.
3. The use of split key encryption entails joint trust in both government and vendor, thought to be unworkable, to achieve some level of assurance and suggests a medium level of expertise and effort and that some level of inconvenience is imposed on users.
4. Th use o n encryption achieves no privacy and security assurance and n expertise, effort, or inconvenience.

Table 1. Efficacy of Encryption Techniques

Cost and Benefit	No Encryption	Key Escrow Encryption	Split Key Encryption	Private Encryption
Expertise	no	yes- medium	yes- high	yes- low
Effort	no	yes- medium	yes- high	yes- low
Inconvenience	no	yes	yes	yes
Privacy and Security Assurance	no	some assurance- Trust in government	some assurance- Joint trust in both government and vendor	yes

PRIVATE ENCRYPTION: AN EXAMPLE

1. plaintext: *software: situation dire*

2. *software: situation dire* in ASCII code
011100110110111101100110011101000111011101100001011100100110010100111010
001000000111001101101001011101000111010101100001011101000110100101101111
011011100010000001100100011010010111001001100101

3. Encrypting and deciphering plaintext and key: *software: situation dire/2015*

plaintext	1.11001E+190	*software: situation dire* in ASCII code
key	2015	
ciphertext	5.50874E+186	plaintext/key
plaintext	1.11001E+190	ciphertext*key

Free Riders: *Benefits and Pitfalls*

Free Riders

From Investopedia the definition of "*Free Rider* is as follows: "*In economics, the free rider problem refers to a situation where some individuals in a population either consume more than their fair share of a common resource, or pay less than their fair share of the cost of a common resource."* The common resource under consideration here is the Internet.

Evidence of Free Riders includes:

- Government and industry ignorance and neglect of Cyber Security
- The growing acceptance of Technical Debt
- Government use of past software research without refreshing software innovation investment
- Government reliance on old style standards
- Government adoption of Open Systems
- Government insistence on receiving government-wide data rights from industry
- Government resistance to private data encryption by industry

Internet Culture

From an Internet with a free spirited culture to an Internet in chaos in a few short decades leaves experienced professionals stunned and the public wary. With a range of root cause explanations from ignorance to neglect to distrust, charting the path ahead is uncertain. With faux experts pressing too confidently for unproven actions, government officials too quickly providing empty assurances, and restless public expecting loss of privacy and fearing loss of identity, there is a swelling bubble of dissatisfaction and distrust. To what extent is Internet use indispensable to performance of the mission?

Ignorance and Neglect

Corporate board members, C-suite occupants, and government executives claiming ignorance of Cyber Security risks, threats, and challenges continue to operate as free riders in the Cyber domain. This ignorance and neglect are often coupled with the stigmatization of the Cyber, software, and technology experts who know things that corporate board members and government executives can never know withou STEM background now beyond their grasp.

Pitfalls

Despite the benefits o free ridership, there are pitfalls. Former New York Governor Eliot Spitzer impaled by emails himself indicated he understood these pitfalls when he stated: *"'Never talk when you can nod. And never write when you can talk. M only addendum is never put it in an email."* Hillary Clinton is learning similar lesson on emails. The advantages of a STEM background cannot be overstated. For these two public figures, it is too late. For corporate board members, C-suite occupants, and government executives, there may still be time... no, not time to acquire a STEM background, but time enough to avoid the pitfalls of the Internet by simply avoiding the use of the Internet for data and information they cannot afford to lose.

Dwindling Government Bargaining Power

Operating under the decades-long assumption of superior government bargaining power, the current crop of government executives continues to overplay its hand with private industry whose business opportunities and conditions of engagement are now far more available and favorable in the commercial domain.Yet the government propensity to operate as a Free Rider in software acquisition is persistent. Most notably the government insistence on receiving government wide data rights continues to be a particular thorn in the side of industry. All this may be stimulating the increase in government Senior Executive Service retirements and departures.

Shifting the Paradigm of Cyber Security Blame: From Supplier to Consumer

Internet Control

The Internet was established to disseminate data and information. The Internet is not equipped to control, secure, or protect the data and information being disseminated. In actual fact the data and information that is transferred about on the Internet is not under control, is not secure, and is not protected beyond th due diligence associated wit backup and recovery operations.

Consumer Responsibility

Responsibility for controlling, securing, and protecting the dissemination of data and information must lie with those who choose to entrust proprietary data and information to the Internet. Organizations have proven that they cannot be depended upon to exercise due diligence with respect to the handling of proprietary data and information entrusted to them. If an organization decides to place its proprietary data and information on the Internet, it must acknowledge acceptance of the risk and take steps to mitigate the risk and its consequences.

Mitigating Internet Risk

The most effective, intelligent, and ethical steps to mitigate Cyber Security risk are an organization policy and assured practice to mitigate Cyber Security risk by taking the following steps:

1. Don't put proprietary data and information you cannot afford to lose on the Internet.
2. For those who do, acknowledge acceptance of the risk associated with Internet use.
3. Encrypt all data and information placed on the Internet. Th us of private encryption fully achieves privacy and security assurance unlike key escrow and split key encryption which entail sharing keys with others.
4. Use three factor authentication to control access to data and information on the Internet:
   - What you have, i.e., card, token
   - What you are, i.e., iris, fingerprint
   - What you know, i.e., password, security question

Recapping Ten Ground Truths of Internet Use

1. The Internet was established to disseminate data and information.
2. The Internet is not equipped to control, secure, or protect the data and information being disseminated.
3. In actual fact the data and information that is transferred about on the Internet is not under control, i not secure, an i not protected beyond the du diligence associated with backup and recovery operations.
4. Cyber theory is not yet proven and understood even by our best and brightest, has not been validated in actual use with empirical data, and is not yet in widespread use by industry.
5. Responsibility for controlling, securing, and protecting the dissemination of data and information must lie with those who choose to entrust proprietary data and information to the Internet.
6. Organizations have proven that they cannot be depended upon to exercise due diligence with respect to the handling of proprietary data and information entrusted to them.
7. If an organization decides to place its proprietary data and information on the Internet, it must acknowledge acceptance of the risk and take steps to mitigate the risk and its consequences.
8. With respect to the public commons, organizations with unattended weaknesses and vulnerabilities actually serve as an attraction, even a magnet, for bad actors making everyone less safe.
9. The most effective, intelligent, and ethical steps to mitigate Cyber Security risk are an organization policy and assured practice to mitigate Cyber Security risk by not putting proprietary data and information it cannot afford to lose on the Internet.
10. For those who do, acknowledge acceptance of the risk associated with Internet use, encrypt all data and information placed on the Internet, and use three factor authentication to control

access to data and information on the Internet including what you have, i.e., card, token, what you are, i.e., iris, fingerprint, and what you know, i.e., password, security question.

Privacy and False Claims: *False Light and Actual Malice*

The result of a shifting definition of privacy and immature privacy practices, an uncontrolled Internet infrastructure and unproven Cyber Security practices, and free riders i free spirited Internet culture has led to frivolous privacy policy assertions, promises, and commitments that border on false claims. The unproven state of Cyber Security protection is well known by the experts in the field and less known and accepted by industry executives. An enterprise whose privacy policy commitments are not matched by a capability to meet the commitments made is presenting itself in a false light and where done knowingly is guilty of actual malice.

Cyber Security: *Fines and Cyber Insurance*

Cyber Fines

Cyber fine imposed on the victim of Cyber incident is straightforward while in fact Cyber Insurance itself may border on the deceptive. Since neglectful and unprepared organizations serve as an attraction to Cyber bad actors and their actions, these unready organizations make the Internet less safe for everyone. While fines may appear punitive, they actually operate as tough love measures that encourage organizations to take the prudent measures known to be effective in order to improve the landscape for all.

Th use o stiff fine for organizations who attract and suffer Cyber attacks through their lack of readiness, especially the failure to adopt a Cyber Risk Management culture, is both necessary and useful.

- *Necessary* because these organizations wit their unattended weaknesses and vulnerabilities actually serve as an attraction, even a magnet, for bad actors making everyone less safe.
- *Useful* because the permissive and voluntary alternative of Cyber Insurance with premium rates calibrated to Cyber readiness and Cyber Risk Management cultural maturity is in a state of failure to launch with entrenched resistance to sharing Cyber incidents and cost data pending indemnification. The Safety Act flirts with indemnification so long as an incident is declared an act o terror. It too i i a state o failure to launch.

Cyber Insurance

Just why doe Cyber Insurance border on the deceptive? Insurance i based on risk, and risk is uncertainty and the prospect for loss or gain depending on the outcome of an event. An industrial strength software risk management practice is one that treats risk as uncertainty and carefully distinguishes risks from the sources of risk and problems. Since risk is uncertainty, the challenge is to calculate the uncertainty of a risk and accept only those risks whose joint probability of occurrence and prospect for loss o gain are prudent choices Thes are considered calculated risks.

The uncertainties associated with a useful and credible Cyber Insurance market are wide ranging and depend on Cyber Security theory and foundations, reduction of theory to practice, the collection and use of empirical practice data, the validation of actual practices against the theory based on empirical data, information sharing, realistic premium setting, informed and trustworthy coverage, and straightforward dollar convertible Cyber consequences. These uncertainties have not yet been reduced to calculated risks. Therein lies the source of the deception.

I the absence of actua answers to th questions suggested by these uncertainties, th undeterred Cyber Insurance advocates are pressing ahead by substituting the soft skill adoption of a Cyber Risk Management culture for the hard facts of Cyber analytics as the foundation for Cyber Security compliance. While a Cyber Risk Management culture may be necessary, it is a partial solution and no sufficien conditio alone withou genuin Cyber Security foundation.

These advocates even resort to extending insurance risk approaches from other fields, such as, flood insurance. Side stepping the hard questions and substituting other paradigms means that the essential Cyber Security foundations will remain undiscovered. Yes, Cyber Insurance approached in this expeditious manner does border on the deceptive.

To what extent can Cyber Insurance also become punitive? Just as flood insurance may be denied to those who wish to build on flood plains, perhaps Cyber Insurance may be denied to the unprepared organization wishing to use the Internet for data and information it cannot afford to lose. So both fines and insurance can come with a punitive edge, and each can serve as a carrot or as a stick.

Cleanroom Software Engineering

Trustworthy Software Assurance
Trustworthiness requires a commitment to rigor in both software production and its verification. Software Assurance demands two capabilities associated with trustworthiness, the capability to produce trustworthy software products and th capabilit to verify tha software products are trustworthy. Each depends on engineering and technology rigorously applied.

The Cleanroom Software Method and Process
There is the need for a rigorously defined Clean Room method and process to produce a provably correct Clean System: one whose method possesses the means to investigate legitimacy, confirm intent and wherewithal of people, verify process execution, and validate outcomes achieved in determining that a legitimate Clean Room was in place and operation and one whose outcome is based on trusted software engineering principles and practices in producing provably correct software components.

The Clean Room Software Engineering Process includes separate teams for Management, Specification, Development, and Certification of the Clean System .
1. Clean Room Software Engineering teams prepare artifacts associated with functional specification, usage specification, increment planning, correctness verification, usage modeling, test planning, statistical testing, and certification (Trammell, C J., R. C. Linger, J. H. Poore, and Stac J. Prowell 1999)
2. The kernel of Clean Room Software Engineering assurance is trusted software engineering using Structured Programming with its rigorous and provably correct use of zero and one predicate prime programs along with proper programs composed of multiple prime programs limited to single entry and single exit (Linger, R.C., H.D. Mills, and B.I. Witt, 1979), (Linger, R. C. and C. J. Trammell 1996).

With the rigorous, defined Software Clean Room method and process specified, the question of a whether a legitimate clean room was in place and operating can be addressed by confirming the equivalency of the intent and means employed, verifying the extent to which the defined protocols of separation were practiced, validating the Clean Room Software Engineering process execution and outcome with respect to convincingly achieving the intended result of a Clean System, and reporting the results in terms of findings, rationale, recommendations, and consequences.
Project Plan: Increments and Iterations
Th first challenge o a Critical Infrastructure Resilience project i to focus o the value proposition and arrive at a comprehensive set of technical performance measurement incentives based on the following assertions and principles:
1. Stakeholders are in agreement and share a vision for the project.
2. An opportunity value proposition has been established, and there is stakeholder shared vision for achieving it.
3 The work product i value add for stakeholders and traceable to user stories and the “done” criteria for the way o working.

The second challenge is to obtain team commitment to systems engineering and software engineering collaboration needed to arrive at the deepest possible user domain awareness across al sectors of the critical infrastructure. This ca be done through early operations analysis, modeling, and simulation in order to integrate the needs of the systems, software, and users in the best possible way. Particular attention is to be paid to sector recovery time objectives and the technical performance measurement incentives to best assure their achievement through system survivability engineering.

The third challenge is to structure the software development plan as an incremental development with well specified design levels and incremental releases each with fine grained cost accounts, formal software inspections of design level artifacts, careful management and visibility of systems engineerin *"to b determined"* items, and a relentless focus on the innovation needed to meet the challenges of resiliency. Th Critical Infrastructure Resilience Way o Working Work Breakdown Structure is shown i Figure 1.

Th fourth challeng is to apply strict accountabilit and control of cost accounts and work packages based on a work breakdown structure and work responsibility matrix. Cross charging is prohibited, that is, systems engineers are prohibited from charging software engineering work packages. Work packages are opened only when the entry gates are either met or waived by explicit decision Work packages are closed only when and as soo as the work package achieves 100% earned value so that un-expended funds in completed work packages is not used to offset work packages that might be over budget. An estimate to complete (ETC) is made for each work package each month. Where actuals to date combined with the ETC for a work package exceed the budget at completion (BAC), a corrective action plan is initiated where possible.

Linger, R.C., H.D. Mills, and B.I. Witt (1979) Structured Programming: Theory and Practice, Addison-Wesley Publishing Company, Inc., 1979

Linger, R. C. and C. J. Trammell (1996) Cleanroom Software Engineering Reference Model, Version 1.0, Technical Report CMU/SEI-96-TR-022, Carnegie Mellon University (CMU) Software Engineering Institute (SEI), November 1996.
http://resources.sei.cmu.edu/asset_files/TechnicalReport/1996_005_001_16502.pdf

Figure 1. Work Breakdown Structure for Critical Infrastructure Resilience Based on Cleanroom Software Engineering Way o Working

Task	Task Type	Situation System	Response System	System Assets
1.Requirements	User Stories			
2. Software System Architecture	Software System Architecture			
3. Project Planning	Increment Planning			
3.1 Design Level Planning	Increment Planning			
3.2 Incremental Development Planning	Increment Planning			
4. Design	Interface, Design, Control, and Usage			
4.1 Level 1 Design	Operating System and Middleware Environment Configuration Specification			

Task	Task Type	Situation System	Response System	System Assets
4.2 Level 2 Design	Intended Function and Persistent Data Specification	Sector Baselines • Intended Functions • Interface Specifications • Recovery Time Objectives	Resiliency Functions • Intended Function Specification • Persistent Data Specification	Intended Function of services and facilities
4.3 Level 3 Design	Interface and Control	Intelligent Middlemen Control Specification	Distributed Supervisor Control Specification	Defense in Depth, Business Continuity, Survivability Services Specification
4.4 Level 4 Design	Usage Specification (Arcs and Nodes Identified)	Usage Specification (Arcs and Nodes Identified)	Usage Specification (Arcs and Nodes Identified)	Usage Specification (Arcs and Nodes Identified)
4.5 Level 5 Design	Usage Modeling (Frequency Annotations on Arcs)	Usage Modeling (Frequency Annotations on Arcs)	Usage Modeling (Frequency Annotations on Arcs)	Usage Modeling (Frequency Annotations on Arcs)
4.6 Level 6 Design	Statistical Testing Design			
4.7 Level 7 Design	Acceptance Test Design			
5. Development	Procedure Development			
5.1 Operating Environment	Operating System and Middleware Environment Configuration Setup			
5.2 Incremental Development	Increment Planning	Procedure Development of Intelligent Middlemen Control • Stepwise Refinement of Intended Functions • Correctness Verification	Procedure Development of Resiliency Functions • Stepwise Refinement of Intended Functions • Correctness Verification	Procedure Development of services and facilities • Stepwise Refinement of Intended Functions • Correctness Verification
6. Test	Statistical Testing and Certification			
6.1 Statistical Testing				
6.2 Certification				

Next Generation Software Engineering

In accordance with the austerity of the times, the immediate goal of practical Next Generation Software Engineering is to drive systems and software engineering to do *more with less... fast* (IEEE 2009). Four practical objectives are identified to advance this goal using smart, trusted technologies:

1. Drive user domain awareness;
2. Simplify and produce systems and software using a shortened development life cycle;
3. Compose and field trustworthy applications and systems from parts;
4. Compose and operate resilient systems of systems from systems.

IEE (2009) O'Neill, D., Preparing the Ground for Next Generation Software Engineering, IEEE Reliability Society, Annual Technology Report 2008, pp. 148-151, June 2009

Conclusion

Just what is the way froward in assuring privacy and security? Keep in mind that privacy is the ability to reveal oneself selectively and security is the condition of being protected against danger or loss. Simply put:

1. Government needs to accept and encourage private encryption and not hold out for key escrow of split key encryption.
2. Government needs to accept indemnification or at least targeted liability to encourage data and information sharing by industry partners.
3. Organizations need to adopt and practice three factor authentication to control access to data and information on the Internet.
4. Organizations need to adopt and practice private encryption of data entrusted to the Internet.

661 words

Don O'Neill Biography

Background

Following his twenty-seven year career with IBM's Federal Systems Division, Don O'Neill completed a three-year residency at Carnegie Mellon University's Software Engineering Institute (SEI) under IBM's Technical Academic Career Program and later served as an SEI Visiting Scientist.

As an independent consultant, he conducts defined programs for managing strategic software spanning competitiveness, security, and process improvement. As an expert witness, he provides testimony on the state of the practice in developing and fielding large-scale industrial software and the complex factors that govern their outcome. As an inventor, he has two patents pending.

He served on the Executive Board of the IEEE Software Engineering Technical Committee and as a Distinguished Visitor o the IEEE. He is a founding member of the Washington DC Software Process Improvement Network (SPIN) and served as the President of the Center for National Software Studies (CNSS) from 2005 to 2008. He is a graduate of Dickinson College in Carlisle, Pennsylvania with a Bachelor of Science degree in mathematics.

Current Research Projects

Don' O'Neill' current research is directed at public policy strategies for deploying resiliency in the nation's critical infrastructure; disruptive game changing fixed price contracting tactics to achieve DOD austerity; smart and trusted tactics and practices in Supply Chain Risk Management Assurance; a defined Software Clean Room Method for transforming a proprietary system into a Clean System devoid of proprietary information, copyrighted material, and trade secrets and confirming, verifying, and validating the results; and a constructive approach to sequencing the transition of SEMAT Essence Kernel Alpha states with an eye to pinpointing the risk triggers that threaten success and lead to the accumulation of technical debt.

Latest Expert Witness

Don O'Neill served as a Litigative Consultant for the Department of Justice in 2014-2015 in connection with false claims where there is the need for a rigorously defined Clean Room Method to transform a proprietary-laden Dirty System into a provably correct proprietary-free Clean System, one convincingly devoid of reliance on proprietary information, copyrighted material, and trade secrets and not considered a derived work.

Recent Book Project

Don O'Neill recently completed his seven chapter contribution to "*Software Engineering in the Systems Context*", ISBN 978-1-84890-76-6, College Publications, Kings College, London, to appear in 2015. collaborative effort among international experts whose mission is to renovate the practice of software engineerin where the situation i dire, the book addresses the frontiers o research in software and the systems that depend on it for global competitiveness and national security.

https://www.linkedin.com/profile/view?id=AAIAAAEjGD0Bj2DsM9unTWlsuTr8OrQZlsWTeI4&trk=nav_responsive_tab_profile