Submission to NIST Draft 2

Framework for Improving Critical Infrastructure Security

Steve Wilson and Peter Coroneos

18 January 2018

We appreciate the opportunity to comment on the NIST draft framework which we regard as a positive step forward in helping secure core infrastructure from current and emerging cyber threats.

This submission is broken down into the following sections:

1. Comments relating to Identity Management & Access Controls (ID & PR.AC)
2. Comments relating to Prevention, Awareness Training (PR.AT)
3. Additional comments
4. About the contributors

1 Identity Management and Access Control ID & PR.AC

One of the most significant extensions of the Framework is the incorporation of Identity Management into the category **PR.AC**. Identity Management (or IdM) is a major growth area for cybersecurity practice, as reflected by initiatives such as the White House's National Strategy for Trusted Identities in Cyberspace, the formation of the Identity Professionals organization IDPro, and NIST's own ongoing development of the *Digital Identity Guidelines* SP 800-63 (previously, *Electronic Authentication Guideline*).

Commentary

We note that the **PR.AC** category has been extended with two more sub-categories **PR.AC-6** (identity proofing) and **PR.AC-7** (risk-based authentication of users, devices and other assets).

Standardized identity proofing (**PR.AC-6**) is a work in progress around the world; NIST will appreciate from its policy mapping work over many years that harmonizing the way different organizations gauge and communicate risk is difficult. Our observation is that risk management methodologies (such as the classic **ISO 31000**) are good for communicating risk within an organization but not between organizations, because everyone calibrates the seriousness and likelihood of threats locally and differently – as they should. In identity management, this makes identity proofing awkward across national boundaries; national digital identities very rarely interoperate, and identity proofing standards such as **ISO 29003** have been painfully difficult to finalise.

Risk based authentication of assets (**PR.AC-7)** is a critical effort in the context of the Internet of Things, as well as the pervasiveness of mobile devices and personal hardware in everyday activities. Efforts to standardise and leverage personal hardware security have made enormous progress, in the GSM Association, and the FIDO Alliance, amongst others. We are particularly impressed by how the FIDO Alliance has "consumerized"

strong authentication to reduce the use of passwords. The FIDO Alliance has been remarkably successful, partly thanks to a focus on the *authentication* layers of the IdM stack where the FIDO protocols standardize how metadata is exchanged about a device's state, certifications, biometrics, location, recent history, and user behaviour. These signals allow applications to make their own fine-grained risk-based decisions about identity. FIDO protocols are now being formalized for unencumbered publication by the new W3C *Web Authentication Working Group*.

Observations

Strategically, FIDO is an example of how identity management practices have evolved to focus less on *who* a user is, than on *what* they are. It is possible now to retrieve all sorts of signals to discern the state of smart devices and their users, and to better manage security. We see attributes as being easier to federate than identities across organizational boundaries; we predict that attributes will become a dominant currency in the digital economy, with new supply chains and business models emerging to deal in and trade verified attributes. There are several worthwhile standardization efforts around the provenance and reliability of attributes, including the IETF's *Vectors of Trust*, and the W3C *Verified Claims Task Force*.

In general, we would like to see the Cybersecurity Framework continue to grow and to reflect these macro trends in the digital economy. The practice of cybersecurity in general (and identity management in particular) seeks to do more than protect enterprises, but to enable new business. Traditional security is concerned with keeping bad actors out, whereas modern IdM seeks to let legitimate actors in, by streamlining and automating authentication and authorization decisions. The collective mindset of the security professional is evolving.

Recommendations

Adding Identity Management to **PR.AC** is a good start, but the Framework needs to do more to integrate the latest developments in IdM practice. At a minimum, the Framework should make more use of NIST's own Digital Identity Guidelines **SP 800-63.** It could also draw on the latest international standardization of identity attributes management in the W3C especially.

We suggest these developments in IdM are leading to more coherent critical infrastructure for the digital economy, where data and vital metadata (about provenance, quality, consent and jurisdiction) are all more widely available from harmonized and contestable cross-sector supply chains.

2 Prevention, Awareness Training PR.AT

Observations

We support the continued general recognition of training and education and the role of human factors as an element of risk.

However, we would like to see greater emphasis in the standard incorporating and reinforcing the language of *behavioral change* as opposed to mere awareness raising.

This is implied in some of the references which the Category references. For example, **CIS Control 17** states: "Perform gap analysis to see which skills employees need to implement the other Controls, and which *behaviors employees are not adhering to*, using this information to build a baseline training and awareness roadmap for all employees." [emphasis added]

While most of the other standards don't specifically refer to behavioral change, **NIST SP 800-53 Rev 4 (2009)** does pick up "rules of behavior" in relation to inappropriate use, but stops short of stating how adherence to required behaviors is to be monitored, measured and where necessary, modified.

Although there is passing reference in a couple of the standards to simulated attacks, ensuring adherence to standards and processes is fundamentally a behavioral issue and will not be achieved by awareness raising alone.

Overall, as we have argued elsewhere, we see the need for a far more sophisticated and rigorous understanding of *why human factors continue to expose organizations and infrastructure they control to severe disruption*.

NIST is well placed to help drive that shift in understanding and the language of the Framework is an ideal opportunity to start.

Discussion

It is our view, based on 20 years of end user education, that awareness raising and education are of limited effect in reducing risk exposure unless we adopt a more sophisticated understanding of why humans continue to engage in risk behaviors even when they may be aware such behaviors are contrary to policy.

The reasons for this are complex, but at least we can say the lack of obvious proximity between cause and effect which might take place in traditional threat environments doesn't operate online, therefore the desired human behavioral adaptation to risk consequence is not likely to respond to simple box checking training exercises.

In the worst case, ineffective training can lead to a false sense of security that human factors have been adequately managed.

Educational psychology has much to say about behavior. Unfortunately, this disparate discipline would not normally find its concepts naturally appearing in cybersecurity literature.

This submission seeks to bridge that divide so that well developed understandings and methods which have applied in education for decades can be introduced, recognized, and more formally accepted in the cyber sphere.

From the psychology literature we see 'behavioral objective' defined as 'a description of observable behaviors that relate to learning.' Notice the use of the term 'observable'. This is relevant to cybersecurity since much of the problem is that the behaviors which are often the cause of the problem are not observed. Specific strategies must be employed with this in mind. A simulated phishing attack is a good example, but in itself will not

modify behavior unless the follow up training is both sympathetic (ie. non-punitive) and transformative. Progress must be monitored, measured, retested and acknowledged.

Behavioral objectives must specify what behavior a subject must demonstrate or perform in order for a trainer to infer that learning has taken place. The use of the terms 'demonstrate' and 'infer' are instructive, for the same reason 'observable' is above– because learning typically cannot be seen directly, therefore the trainer must draw inferences about learning from evidence they can see and measure. We note that bodies like CIS and the SANS Institute have shown a preference for change that is measurable, so these points should be uncontroversial, and likely welcomed.

If constructed properly, behavioral objectives provide a basis for sound education and the development of metrics. This approach takes us beyond the awareness raising platitudes of 20 years ago, and into realms where inferences that the requisite change has taken place can be reliably drawn. If successful, the organization becomes safer through a reduced human-induced threat posture.

Recommendation

That the language of **PR.AT 1** be strengthened to recognize that an effective cyber-security training specification will:

- Identify which specific behaviors need to change
- Use methods which are behaviorally based
- State how the change will be measured
- Explain what action will be taken to ensure risk behavior is identified, and where necessary remediated.

The draft **PR.AT** category description currently reads:

> *The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.*

We would respectfully submit an amendment* as follows:

> *The organization's personnel and partners are provided cybersecurity education which is behaviorally based and identifies measurable outcomes to ensure performance of their information security-related duties and responsibilities is consistent with related policies, procedures, and agreements.*
>
> **Consequential changes may be needed to **PR.AT.1–5** to echo this approach.*

3 Additional comments

Issue: The use of the word 'statutorially' is redundant in referring to changes implemented by the *Cybersecurity Enhancement Act 2014*

Reason: All Acts of Congress are statutes therefore changes introduced via legislation are necessarily statutory. The word adds nothing to the meaning of the sentence.

Change suggested: Delete the word ‘statutorially’ on lines 95 and 161.

4 ABOUT THE CONTRIBUTORS

Peter Coroneos

Peter Coroneos is an internationally recognized thought leader, pioneer and advocate for best practice in cyber safety. He was twice invited to the White House to advise the Obama Administration on cybersecurity policy. His area of special interest is the design and implementation of safer online practice as part of the broader *trust imperative*, which he maintains is not only essential for the internet, and also for societies at large.

In 2012, he was invited to brief officials of the US Senate Committee on Homeland Security in relation to industry led best practice in cybersecurity policy. He has also briefed officials from the US Commerce Dept, Department of Justice and Homeland Security.

His analysis and commentary have been widely reported internationally and he has delivered presentations and keynotes on five continents. He has given expert testimony on cyber issues to numerous Senate and House Committee inquiries and has briefed governments of US, UK, Canada, the EU and New Zealand on initiatives he developed while leading the internet industry in Australia. Some of this work formed the basis of initiatives replicated elsewhere, including the US.

He is currently Regional Head APAC for the Cybersecurity Advisors Network (CyAN), a Paris-based global NGO representing cyber professionals. He is also Principal Advisor, Coroneos Cyber Intelligence, providing strategic advice to business and government on cyber threats.

Peter formerly served as Chief Executive of the Internet Industry Association, Australia's lead trade association from 1997 to 2011, where he pioneered numerous initiatives directed towards increasing online trust and safety.

In 2010, he led the development of 'icode', an international model of best practice for malware mitigation on ISP networks, which, with White House support, drove the development of the FCC-endorsed CSRIC code announced and implemented in 2012.

As part of bilateral US-Australian collaboration on Critical Infrastructure Protection, Peter was nominated to lead an industry delegation to Washington at the invitation of the Australian Government in joint talks with leading law enforcement and national security agencies, post 9/11.

Well versed in standards development, Peter steered or directly contributed to the:

- OECD Guidelines for the Security of Information Systems and Networks and
- AS/NZ IS Standard 270001 (equivalent to ISO 27001)
- Self- and co-regulatory codes of practice in areas ranging from privacy, cybercrime, child protection and spam.

Steve Wilson

Steve Wilson is a researcher, analyst and innovator in privacy and security, and one of the world's most original thinkers in digital identity.

In 2004, Steve established the independent Lockstep group in Australia, which provides strategic analysis and advice in cybersecurity and privacy, and researches and develops disruptive identity management technologies.

Since 2013, he has held an adjunct position of Principal Analyst at Silicon Valley-based Constellation Research, he leads the Digital Safety and Privacy body.

Steve is an active member of the international security and privacy communities. He is a founding member of the Identity Professionals Association, and the Australia-New Zealand chapter of the International Association of Privacy Professionals (iappANZ).

He has recently been nominated to the Advisory Council of the US National Strategy for Trusted Identities in Cyberspace (NSTIC) and over 2011-13, he sat on the NSTIC Privacy Committee. Steve has also recently been endorsed for membership of the Cybersecurity Advisors Network (CyAN).

He is currently a member of the program committee for the "European Integration and Democracy" series, and since 2016 has been Privacy Track Chair for the Cloud Identity Summit. He is a past member of the Australian Law Reform Commission's privacy reform technologies sub-committee.

His clients have included:

- US Department of Homeland Security
- Digital Transformation Agency (Australia)
- Biometrics Institute
- FIDO Alliance
- IBM
- Infosys
- Persistent Systems
- Aetna
- Pharmacy Guild of Australia
- Australia Post
- Australian Passport Office
- Australian Attorney Generals Department Face Verification Service
- ASEAN
- World Bank
- Governments of Hong Kong, Indonesia, Kazakhstan, Macau, Malaysia, New Zealand and Singapore.

Steve is currently undertaking a PhD on the evolution and ecology of digital identity, at the Australian Defence Force Academy, Canberra.