Open Standards

David O’Berry
Director of Information Technology Systems and Services, South Carolina Department of Probation, Parole and Pardon Services (SCDPPPS), Columbia, South Carolina, U.S.A.

Abstract
This entry offers scenarios, along with how and why a newer, quicker, more open standards process matters from a practical application standpoint.

From an information technology (IT) security perspective, the real world has changed so drastically in the last few years as to make an entry that describes “practical” thought processes with some real implementation considerations valid and therefore worth your time. This entry will not be like many of the entries in this encyclopedia in that it will ask you questions as well as proceed in a conversational style that may be disconcerting for some. Due to size restrictions, some concepts may simply be touched on while others may be more fully explored. To be clear, none of this is groundbreaking, and in reality there are probably very few original concepts that I will write about. What I am hoping to do is frame up the real world through a brief synthesis of existing ideas in hopes of encouraging a larger number of practitioners of our discipline to move back to some type of significant leadership role in this environment. Ultimately, instead of being herded, we can lead and be led by things that apply to what we are seeing right now instead of 5 or 10 years ago. In order for us to get to that point, we need to understand where we came from as well as some of the possible paths we have ahead of us.

WHAT MATTERS

All too often in IT, specifically in security, we get so inundated with the “wheres” and “hows” of something that we tend to lose sight of the real “whats” and “whys.” Holistically speaking, the practice of security is one that everyone can subscribe to, but the realities of the world we live in is that practical application is something very few of us actually want to take on. Having said that, the real challenge that IT has had in the past, not specific to security, is a lack of customer-based leadership in what is going on at any given time. We have often allowed the vendor brain-trusts in one form or another to be the guiding light because, let’s face it, in many cases those guys bring a lot of incredibly smart minds to the table, have patents, and do wizbang things that amaze us. An unfortunate side effect of this is that we oftentimes allow ourselves to be cowed by them. They then get us in a situation and run a whole team of “ninja monkey engineers” at us that have every reason in the book why their product is far, far better than any other product and why we should buy only from them, asking us to barely give any consideration to what else is out there. In many cases this has even contributed to the concept of IT for IT’s sake, which has then created tension between us and the business. What we have to remember is there are no IT projects—there are simply business projects with IT components. Yet, in the past, we have forgotten or at least strayed from that tenet that makes us ripe to be divided and conquered by vendors that need our dollars to survive.

Now, how often is the product by that single vendor you tested actually the best thing out there to solve the problem occurring in your organization? While the statistics vary depending on what source you reference, there is no question that far more products and companies are actual flops than successes. The reality is, that’s how it’s supposed to be really, because if everyone’s idea was the best idea we would be left in intellectual gridlock. So what we have is a situation where more failures than successes are the true path to progress. The real problem is that instead of seeing this, we get this marketing blitz that tries to convince us to buy their product because their “ninja monkeys” actually get it right while these other vendors are supposedly just confused and bumbling around with no hope of finding salvation. Sound familiar?

It should sound familiar, because that is how the industry has worked for many years. That’s certainly not a new thing and, especially in the initial phases of computing, was not necessarily a bad thing. However, as the stakes have been raised it has increasingly become evident that we have got to change our way of thinking. We cannot afford to wait anymore as these companies continue to slug it out to control what should be agile rapidly evolving open standards that we require to even have a remote chance of stepping away from the edge of the digital abyss at which we stand. What do I mean by that? Well, for starters we are in a digital ecosystem unlike anything
we have experienced at any point in human history. It is the concept of the “circle of life” but it is happening at warp factor nine and, to the chagrin of some, it is driven by users. Yeah, those horrible plankton-like creatures (joking here) are what feed the entire world because they are what matters. They are the iPhone Gremlins, Skype Monsters, Gmail Maggots, and Streaming Media Punks; those little malware-infested pod people are why we do what we do. These new generation of millennial “I GOTA HAVE” end-users are a critical component of the engine that will drive the world economy forward in the next half century. Scary, isn’t it? It does not have to be. At every turn we have to remember that business functions best based on efficiency, and these people that our industry has tended to look upon rather disdainfully at times are the lifeblood of each and every organization. That graphic artist that is so special that he has to have his own Mac is there for a reason, and it is to pay your salary, because in most cases what we do has no directly visible positive impact to the bottom line. That goes back directly to the purpose of IT and IT security as enablers for the business and not entities unto their own selves. I know what you are thinking and sure, we help the bottom line not become a negative, but let us be realistic: We know how hard that is to explain to people.

Why is that? Why does something that matter so much to individuals and companies seem so arcane? Why does it sometimes become such a chore to even attempt to provide a value proposition for what we do? For starters, it is hard to explain something that the world as a whole has taken very little vested interest in until it is almost too late. As a profession, you know that those of us who have been talking about the challenges coming have been in the minority quickly drowned out by the folks who tend to point to Y2K as some horrible failure because we did our jobs so well that nothing much happened. That may be counter-intuitive, but from a practical point of view, it is often how the real world functions. Often these same professionals, as well as some of the vendors we deal with, get such tunnel vision that it looks to many of us like they have “Ostrich Syndrome” with heads so firmly buried there is no hope of illuminating the way to “truth.” It sounds hopeless, but it is not. It just takes a different mentality and way of thinking that starts with customer-driven standards that move faster than the existing process. Going forward, it is my contention that standards-based interoperability is critical to network security with empowered users actively participating in driving those standards rather than passively allowing vendors to continue to control the process.

**WHY IT MATTERS**

Let us look at it in a different light for a moment. Do the various branches of the United States military usually wait for vendors to come tell them how and what they need to fight the next war? No, they do not. Instead they go to the vendors, they work together to determine what makes sense, and then put their combined knowledge and experience to use accomplishing incredibly important goals. For the most part, our industry operates almost completely opposite of that model usually driven by vendor’s product cycles. The problem is now it is no longer practical to continue down that path. The reason the old way no longer works is that now we must contend with threat cycles that spin at a much more rapid pace than existing product cycles could ever hope to move. A simple graphical representation is given in Fig. 1.

What does that mean? Well, for one thing, by the time a product gets through a vendor’s cycle and actually makes it to market, the real world needs of the customer have more than likely changed. So while we are waiting...
through the starts, stops, and failures that I reference earlier as the standard way things progress, we are locked in a death-spiral as new problems hit. We all know that the real world issues stem from design challenges that often had security in the backseat (at best) early in the formative years. So now, the bolt-on thing keeps occurring over and over again, and vendors at times sell us bad code to protect worse code. But wait; there goes that counter-intuitive thing again. So how do we even begin to dig ourselves out of this situation? Well, the first step is to understand the gap between education and innovation in our society. We must also recognize that while luminaries from the vendors have generally led in the past, this does not have to be the case. In fact, it should not be the case in the majority of areas once we solve the education and communication aspect. We need to remember that open standards that evolve fairly rapidly are critical to this equalization of the customer/vendor relationship. They can contribute to a paradigm shift as entities of all sizes, from the incredibly large to the very small, are involved in a process that has too often been “big vendor and friends” only. I will touch on these topics plus some practical thought processes for design concepts in the next few pages.

STANDARDS—PART ONE: REVOLUTION, NOT EVOLUTION

I have discussed standards and their importance in the generic sense up until this point. Now I am going to discuss a couple of scenarios over the next few pages along with the how and why, in my opinion, a newer, quicker, more open standards process matters from a practical application standpoint.

We are all aware of the rapidly evolving security landscape and in many cases it stems from the confluence of vast amounts of computing power coupled with faster and faster ways of communicating. This creates some crazy good opportunities for businesses in all fields to leap forward and to really prosper. All facets of the economy have been affected by this “digital industrial revolution.” It shows in many positive and also many negative ways. As with any revolution of sorts, there is collateral damage in many forms, and right now what we are dealing with is an older security posture with very new threats. Increases in bandwidth together with the ubiquity of attachment points left many people looking around trying to figure out how exactly to stem the flow of data to areas they were not prepared to protect in the early to mid-2000s.

With that in mind, now we have to look at ways of gaining comprehensive distributed visibility across the enterprise while at the same time processing more security event-related information than people have the stomach to deal with at this point.

We all remember the intrusion detection system (IDS) scenario where at least one major pundit-filled analyst organization called the solution dead before it got fully implemented, based on false positives and what they felt was a uselessness of after the fact information. Of course, that gave way to the newest marketing phenomenon, intrusion prevention systems (IPS), and while that stays in effect today, many vendors initially just took their old IDS systems and called them IPS while giving them some blocking capabilities. This is a standard Marketing 101 trick: “Why invent when you can rename?” To be fair though, that is not a vendor only problem and in many cases IDS (when coupled with the proper configuration and education level) did, and still does, serve a purpose in many organizations. The challenge was also with organizations finding the people to run the systems or finding the money to educate on it. Both of those are not really vendor problems and so fall on organizations that see those types of things as just “line-item security issues” that can be cut the same as office supplies.

I grew up in a small individual computer world for the most part, starting back with the VIC 20 and Commodore 64, graduating to the Amiga and then the PC. When I look back I am always astounded at what we were able to accomplish back then on so little real estate versus what we can accomplish now with computers that simply dwarf those machines. As we began to connect those IBM PCs, the power of data-sharing really began to manifest itself and the world was a happy place. There was free flow of information, shared printers, and consolidated points of storage that did not cost millions of dollars. Businesses were in heaven and security was a real afterthought, because in the world of small disconnected PCs the mentality was far different than it had been working from the center out, the way mainframes functioned. Today, some organizations are swinging the pendulum back toward centralization with the thin client concept but we cannot ignore endpoint security. Infected endpoints can capture passwords and confidential data and mount attacks on critical systems. We really need trustworthy devices, whether through the use of hardware security like the trusted platform module (TPM), software security, or more likely a combination of the two.

While the concept of the “centrally distributed” computing model is fairly simple, what is not simple is the evolution and implementation of the idea. The seemingly contrary concepts of power at the edge and control at the center really make for a significant set of challenges. Addressing those things has often been the purview of the vendors and we have at times been forced to take a backseat and watch as each successive product has rolled out hoping for our chance to “get it right.” The problem again comes back to the product cycle versus threat cycle issue and it has become more
and more apparent over the last 10 years that the traditional vendor-centric model just cannot work without modifications. Enter open source and the concepts of development communities and others that now have different motives to create products and services. What that has created is a unique opportunity to potentially bring in the vendors we are used to dealing with and communities that are relatively new to create a workable yet completely untested paradigm shift to heterogeneous open interoperability.

STANDARDS—PART TWO: FOUNDATIONS FOR VISIBILITY

It is only relatively recently that there has been real hope, in my opinion, for a fix to this situation that will not have to be brought on by a catastrophic failure that requires government intervention, regulations that will stifle innovation, and more fear and paranoia than is healthy for the participants in this global digital ecosystem. The old hardened perimeter is passé now with people calling for “deperimeterization” or whatever they choose to call it from week to week. “Defense in Depth” versus Mothra—many innocents in danger! So what is the real deal with the existing state? Well many companies have now recognized that security has to permeate what they do in order to have a chance at succeeding.

How permeation occurs is open to interpretation but the real problem comes in the fact that over the years very little heed has been paid to the security aspects of the frameworks and code that really are the foundation of the environment. First and foremost that has to be fixed, and organizations such as the International Information Systems Security Certification Consortium (ISC²), Information Systems Security Association (ISSA), ISACA, and SANS are concerning themselves with at least discussing and possibly helping people to understand and hope to follow, test, and certify secure coding methodologies that will fall off in years to come. We even see large companies getting into the mix with Google, Microsoft, Sun, IBM, Oracle, and others preaching the virtues of writing good secure code while providing guidance within their own spheres of influence. The challenge is that in the interim we are not there and until we get there we need to bridge the risk gap in order for the digital ecosystem to continue to function properly.

To have a shot at really making a dent in the problem, we have to go back to standards, interoperability, and the leadership aspects that have been previously referenced. At this point organizations like the Trusted Computing Group (TCG) have in place various working groups that have responsibilities for many of the most at-risk areas of computing. The standard frameworks put forth by an organization like the TCG in an area like Network Access Control cannot really be overstated because the baseline security posture of many organizations is simply not where it needs to be. Going back to the ecosystem analogy, each of these organizations that are deficient can directly impact even the healthy organizations by becoming jump off points for attacks of various kinds. It is not unlike the human immune system in that a breach in one area threatens the entire organism. Another way to think about this is the “Digital Feudalism” concept and how in many of the older security models we have each gotten in our castles with our moats while peering out waiting for the horde to attack. Unfortunately, things have changed drastically and now the malware horde is even recruiting people within the castle to work from the inside out and we all know that it only takes one internal challenge (the horde recruiting one of your own) to make us vulnerable to all sorts of problematic issues.

From the design perspective it seems almost impossible to stop the threats without becoming restrictive to the point of complete uselessness. Throughout my career I have been down both roads (wide open and steel jaw shut) and I will tell you that with the new generations of users coming, and understanding what is really best for the businesses, there is no way to be closed up completely. One of my favorite lines in the movie Jurassic Park is where the scientist alludes to the fact that “nature will find a way” and that really holds true intentionally or unintentionally for both users and the people who want to take advantage of those users. All is not lost though, because over the past couple of years things in security have gotten markedly better on some fronts. The increasing adoption of Trusted Network Connect (TNC) standards should allow us to easily detect infected machines and raise the visibility from the edge. Microsoft’s move to include TNC support in Windows Vista and Windows XP SP 3 and their publication of hundreds of Microsoft protocols on MSDN in early 2008 are positive moves that should be emulated by others. In Fig. 2, you see a logical mapping of real world capabilities that have now been vetted in whole or part by the Trusted Network Connect (TNC), Internet Engineering Task Force (IETF), as well as large multinational companies like Microsoft, Dell, Intel, Hewlett Packard, Symantec, and McAfee.

STANDARDS—TRIPLE PLAY: ENDPOINTS AND FLOWPOINTS AND THE THREAT STATE DATABASE

The challenge of the “power at the edge, control at the center” mantra is in how and where we deploy our
protections. The “Endpoints and Flowpoints” concept is a fairly generic way of describing a defense in depth or “Flex Defense” concept that can adapt as we go to solve the many and varied attacks that we will continue to see. The best way to think about this is that you cannot dam the Mississippi River but you can dam some tributaries while you watch the Mississippi. What that means is that as endpoints come on the network we need to be able to take postures on them that we can then correlate with policies and behaviors. There have been some fascinating developments in this area, both in proprietary products and through open standards like IF-MAP. This new standard allows a wide variety of network security systems (NAC, IDS, DLP, etc.) to coordinate and communicate critical information, building a “Threat State Database” that shows the status of all users, devices, and suspicious activity on the network (see Fig. 3).

By sharing this information, suspicious activity can be correlated with users to identify abnormal behavior and take corrective action. This sort of correlation and communication among network security devices using open standards is long overdue. Longer term, the standards-based participation of the endpoints themselves in the security of the network around them has to be carried forward in a way that they participate more in discerning what others are doing rather than being solely concerned with what they are doing locally. At every juncture, we need to be watching what is going on in the network with tools like sFlow in switches, NetFlow in switches and routers, developing SDKs for switches and routers that allow for open-source

---

**Fig. 2** A logical mapping of real-world capabilities that have now been vetted in whole or part by the TNC and the IETF.

**Fig. 3** The logical makeup of one available set of standards that could be used as a foundation.
innovation, and network visibility servers that can take in data to assist us in determining where we need to put our resources at any given point. While some of this has been around for a while, the deployment aspects of it have become a more complete picture as more and more companies seek to participate and are given that ability by the increased openness of many of the aspects of the community.

What we saw in the past with mostly signature-based mechanisms was an overwhelming of the networks ability to respond. Unlike the normal immune system in a human that generally only responds when a true threat exists, the various network visibility products in the past would simply inundate the security folks with warning after warning. It becomes the “boy that cried wolf” and then things simply begin to be ignored. In an analogy all of us can understand, we may respond to the first 5000 inconsequential Blackberry buzzes but that second 5000 have a high chance of not even raising an eyebrow. Instead, we need to be looking at visibility points along the way that then can trigger responses that begin to capture a lot more information at the first hint of trouble. Distributing some of that open reporting capability all the way out to the endpoint is where I think we will go because while the endpoints have clients on them that protect them, many times the challenge is how the proprietary systems often treat as nonexistent the warnings that come about violations that are not deemed critical. Host-based firewall data goes into the bit bucket from the view of the network as a whole, when it could possibly flow up into the centralized network visibility server to become part of an overlaid “threat state database.” The evolution of something like this could be enterprise first, and eventually could be shared if the communication aspects continue to open up over the next few years. The SETI model with thousands of individual clients participating in a grid working on the distributed task of searching for extraterrestrial life makes a lot of sense going forward especially with the advent of technologies like Common Uniform Driver Architecture (CUDA) and the potential substantial extra processing power it brings. Looking at security in that light, we can see open source clients (there are already several out there for various capabilities) that could then become individual sensors from a network data perspective. This type of distributed peer review could then become an indicator on the network that gives some idea of the danger level based on what the individual clients see around them moreso than actually what they see on them. It would not be a stretch to consider weighting this input based on what we acknowledge to be “known good” endpoints or beacon/buoy machines on the network. The end goal would be to attempt to be able to create a “Federated Security” concept that gives us a whole picture of our enterprise (even a fuzzy one at first) but that allows us to quickly focus the magnifying glass when an area becomes a concern (Robert Whiteley, Forrester Consulting). Eventually the feedback loop for the network needs to follow more along the concept of Boyd’s Loop or OODA Loops that give us an overall more effective activity cycle than simply putting out fires. Refer back to Fig. 3 for an illustration of the logical makeup of one available set of standards that could be used as a foundation for this next iteration of network capability.

Basically in this environment, we are watching the sampled data at different points in the system and as heuristics continue to evolve, we can decide whether or not to focus the more intensive capabilities of the forensic aspect of that network on our trouble spots. With the proliferation of headless attack vectors like printers, iPods, and iPhones, there has to be a way of distributing the load of the visibility so that we have early warning indicators before things overwhelm the core. It has been proven that core defense simply does not work because of the drastic increase in bandwidth coming from the edge, the huge liability located in the endpoint including what data it sees and what it does with that data, and new valid “malware-like” software that serves valid business purposes while fraying the nerves of the security team. As we continue to move toward the evolution of more transient and distributed network security supplicants on these clients, we need to concern ourselves with network design that allows for the inclusion of this data in real time so that when it does get here we do not have to rip and replace yet again. Buying switches that are sFlow capable should be on the agenda while paying attention to both standards adherence in the past as well as roadmap postures for the future again comes to the forefront. Paying attention to how a router supports NetFlow and whether or not the company is really participating in the standards associated with communications in general should become a main criterion for our discussions. Recognizing how we are going to put that information to use and what we need to do in order to further the evolution of the industry needs to become a prime consideration if we are ever to get ahead of the curve.

**STANDARDS: WHY DO THEY REALLY MATTER GOING FORWARD?**

Simple concept: require standards. Right? Well, yes in theory. When we just say it out loud it sounds not only simple, but effective, and just plain makes sense. At the same time what we have found throughout the evolution of this industry and our profession is that the evolution of standards is nearly the sole domain of the vendors. If you think that seems backward then you are absolutely right. It goes directly back to both the “ninja monkeys”
issue as well as the fact that the vendors have a ton of very smart people working for them. By no means am I saying that vendors are all evil. I am just saying that their goal is not an altruistic one by and large. Their goal, in most cases, is to make money for their business while doing no harm to the general public. That is a worthy goal and not one that I am condemning them for in the least. I am simply saying that it is not the goal of IT security, and awareness of their goals and objectives brings power to us and by the transitive property our organizations.

I wrote a brief column about this a few months back and will use some of that here because I have a real conviction about this topic (O’Berry, StateTech Magazine Jan/Feb 2008). I believe that what it really boils down to is that it is time for us to participate in the maturation of the industry instead of just watching as it evolves. One way to do that is to push vendors to abandon their proprietary technologies and demand they support open standards and frameworks. For the past decade, large companies have wagged the dog by manipulating, wasting time, and, in general, simply not allowing the industry to standardize in a timely manner. Some of the largest vendors have opted out of standardization efforts in hopes of forcing people to choose their technology, thereby locking out competitors and locking in customers. Many might say this is a valid business practice, and in the past it might well have been, based solely on a dollars-and-cents perspective. That era has passed, and the future should belong to open, nonproprietary, and scalable solutions because things are too important at this point to leave to simple market chance.

As mentioned earlier, security threats are evolving at an incredibly rapid pace today, which leaves us no real time for the old slow, painful, politics-filled standards process where the incumbent vendors drag their feet until they are forced to the table by market pressure. We have all witnessed the battles over standards such as OSPF, LLDP, IGMP, SMI-S, SFLOW, AVDL, and most recently Cisco NAC/TCG TNC/IETF NEA, and Microsoft NAP. From these various struggles, we have become familiar with the concept of vendor lock-in and defacto closed standards. Concurrently, the game and stakes have changed considerably for everyone involved and we are nearly overwhelmed at every turn by the complexity of handling security in our heterogeneous environments. The previous combination of factors creates a completely untenable situation for the entire “Digital Ecosystem” as a whole. It creates an environment where rapidly evolving user-driven open standards is possibly the only valid solution to step into the breach.

While the standards scenario is a seemingly obvious one, it has eluded our profession in many cases. What has instead happened in the past is at critical junctures where more pervasive open standards might take hold, threatened vendors ramp up the attack, and their engineers and sales people keep coming fast and furious. That causes some of us to feel powerless and therefore give up. Those casualties within the practitioners creates additional gaps based on the silos that they attempt to keep us in and then the pendulum swings even further against the practitioners as those left are fighting increasing odds against not only vendors, but the pundits that tend to push those vendors for money. What we fail to realize is we do wield a great deal of influence if we band together. In my opinion, it is time to stand up as a profession with one voice and say to the vendors we support with our dollars, “do what is right.” It is time to stand up and say that we will no longer allow the tail to wag the dog. At every juncture, we must demand aggressive support of open standards and push vendors to not only participate in organizations like The Open Group, OASIS, the Trusted Computing Group, and the IETF, but to also openly embrace and really contribute to organizations like them. To find our voice, we need to break through the communication silos that have been built around us and find new ways to share ideas and concepts with one another. Those different mechanisms exist now in many fragmented forms and new ones like demandstands.org are coming with the goal of pulling the various pieces together into some type of workable plan that will contribute to an overall global information system transformation.

In the meantime, we must question road maps and require that the vendors we choose to patronize are not only endorsing, but supporting and truly embracing open standards that will encourage the sharing of information, as well as the interoperability of heterogeneous pieces critical to our foundations. It is time for our profession to take a leadership role in our dealings with vendors and their products and interactions with one another. It is time for us to act before we are told we should do something by the very people who then want to sell us the tools to do it. It is time for a greater percentage of IT leaders to come from within the consumers of the technology rather than the purveyors. In order to do that we need to do our homework on each piece of our network to know what standards are necessary. In doing this we can take on various aspects of the product knowledge process collectively while making it clear what we will and will not stand for from the people we choose to do business with. At the same time, we need to consider stronger language in our contracts; “This procurement is contingent on adherence of this product to standard ‘x, y, z’ with the understanding that a lack of compliance by ‘such and such date’ will be grounds for a full refund of purchase price.” Why do we need to take such an aggressive posture? At this point we have ubiquitous access from a steadily multiplying number of devices with rapidly evolving threats that increase in both numbers and complexity every day. The attackers have revolutionary new tools to deliver these threats. Considering all we are
up against, we have no choice but to take issue with
defacto standards and large vendors whose opposition to
open standards kills us from an agility perspective. To put
this in perspective we need to look at the network access
control market and think about how many years it has been
since a valid standard with multiple vendors supporting it
has been in place. It is more than 2 years and yet it is still
an issue. Why? Again, old standards processes where large
vendors drag their feet are simply not reasonable any lon-
ger and at times step in the way of us protecting the
shareholders and customers for each organization. It will
not be long before the issue of public trust rears its head,
which will at that point involve various governments step-
ing in and making life (by accident, of course) very
difficult. Instead we need to get out ahead of that because
the stakes are significantly higher now especially as it
relates to data security. Earlier, standards adherence
mostly centered on efficiency concerns but now it is sys-
temic safety with each entity bearing a responsibility to
the whole. That is a completely different level of responsi-
bility and one that I do not believe vendors really want to
truly acknowledge.

I briefly touched on the concept of “Endpoints and
Flowpoints” and how with the incorporation of the new IF-
MAP specification, we can really begin to have a valid
shot to ingrain security as the network rapidly expands.
We know the ways of the past simply did not scale and
things had become nearly unmanageable with older tech-
ology. In order to move forward, adopting open standards
based frameworks will be one of the most effective and
efficient ways to get an agile, scalable, modular, distrib-
uted security architecture that is truly workable for the
masses. Again, if we look at it with a human immune sys-
tem concept in mind, basically we are all part of one
organism in this digital ecosystem. Slow adaption and lip
service to open standards, as previously mentioned, now
not only affects efficiency, but also affects safety because
if the extremities get an infection it can easily become sys-
temic. While in the past we could just worry about the
security of our organizations and even just the core of our
organizations, this is no longer the case. Again, the prac-
tice of “Digital Feudalism” with the lords of the land
retreating to their castles and pulling up the drawbridge
while peering out from the throne room has seemed poten-
tially reasonable in the past. Now, not so much because we
realize the barbarian hordes (botnets, etc.) really can and
are drafting our peasants, dogs, cats, etc., into service for
use against us.

CONCLUSION

Contemplate this question: When the vast majority of
the digital ecosystem is owned or completely broken
including the very drivers of the financial/economic
food-chain, where will that leave the world as a whole?
Considering this question, and with everything I have
written into consideration, from a “state of stand-
dards” perspective, you have to now ask yourself: “Why
does the tail continue to wag the dog?” Do we deal with it
just because it’s always been this way? Are we going to let
this state of existence continue? Can we afford to do that?
From my perspective, that state of existence cannot and
should not be acceptable going forward. Instead, as men-
tioned, a consolidated voice is required to make changes in
how future critical standards evolve. Our future must
include open security frameworks that allow plug-ins for
innovation with rapidly evolving workable standards, not
only requested but demanded. As individual practitioners
we need to require legitimate road-maps, timelines, and
milestones for standards in the products we use, while con-
tractually requiring adherence by specifying when we
expect open standards compliance and what the conse-
quences are for failing on that front. Keep in mind that this
is not being difficult no matter what a vendor or business
unit says, because more rapid adoption of standard security
frameworks opens the door for innovation both in our pro-
fession as well as the business as a whole. Blind adherence
to a monoculture is neither feasible nor healthy going for-
ward in any facet of our networks and businesses. Being in
the security field, I am sure that those of you who have
read this far realize that easier is not always better. Homo-
egeneous is not practical at this point and each and every
decision we make goes directly to the bottom line of our
organizations, either positively or negatively. Our deci-
sions are not made in a vacuum and there is no doubt that,
in the future, things are likely to get tougher before they
get better. With that in mind, we have to advance changes
that matter at every opportunity we are given.

There are a great number of things that I have either
just briefly touched on here or simply not mentioned
because to do so would extend way past the scope of
this entry. If you get nothing else from what I have writ-
ten, then I hope that you realize that the information
security field has changed rapidly over the last few
years mostly because of just how young it is in the
scheme of society, and it requires a much different
mindset when looking at implementation principles
going forward. As a profession, we need to think outside
the box about how we can begin to affect changes to
the old way of operating. Finally, we need to make sure
we consider how we take things on, what we take on,
how we lead, how we educate, how we drive, and then
adhere to open standards, how we support groups like
OASIS, The Open Group, and TCG, and how we sup-
port concepts like demandstandards.org while clarifying
what we absolutely require of vendors. It is a tall order
but one that I know we can fill if we communicate and
support one another irrespective of old roles, titles, and
predispositions going forward.