Whitepaper

Top 10 things you need to know about how to damage-control both hacker pivots and insider leaks both in enterprise IT and the internet of things.

This whitepaper discusses the top 10 things you need to know about how to damage-control both hacker pivots and insider leaks both in enterprise IT and the internet of things. To frame the discussion, the whitepaper first explains how hackers typically enter their target organization and then move laterally ("pivot") on to valuable assets.

It then explains how most organizations are overwhelmed, understaffed and/or underfunded when it comes to cybersecurity. These constraints create a critical need to prioritize on the most critical cybersecurity measures. However, often these priorities are unclear or hard to determine, leading to less-than-optimal cybersecurity product purchases and/or activities. This is because the metrics about which overarching cybersecurity priorities matter most are by-and-large not well-established or well accepted by the cybersecurity industry – making it very difficult for customers to know what to do first and what is a "nice to have".

For sake of simplicity (and a catchy title), we will refer to those priorities as "the top 10 things" to do to control and monitor hacker pivots, and accidental or malicious insider leaks. It is not the primary purpose of this whitepaper to postulate a top 10 list, but rather to discuss the needs and challenges to get to industry-wide vetted metrics of what matters most in cybersecurity (potentially with some adaptations based on industry, IT landscape, regulatory/legal environment etc.) Instead, the primary purpose of this whitepaper is to nudge the cybersecurity industry in a direction where customers can decide based on clear metrics where they should put their priorities, rather than leaving customers in the current state of confusion caused by the noise created by the Cybersecurity industry.

Dr. Ulrich Lang
Founder & CEO
ObjectSecurity
info@objectsecurity.com

Contents

objectsecurity.com
@objectsecurity

Whitepaper

Top 10 things you need to know about how to damage-control both hacker pivots and insider leaks both in enterprise IT and the internet of things.

Introduction: Why does this matter?

Don't we already have this problem solved? Clearly a lot of time has been spent by various organizations to come up with 10,000's of controls in hundreds of frameworks, guidance, regulations, standards etc. Just to name one prominent example, there is the NIST 800.53 guidance (discussed further down), which lays out in hundreds of "controls" what US government entities should do to implement cybersecurity.

However, anyone who has tried to implement cybersecurity across an organization has likely experienced that there are too many topics to cover, and there are no good sources to explain what the top areas to focus on should be. In fact many players in the cybersecurity industry's "marketing machine" spend considerable effort to sell customer on one kind of product or another, without really helping customers with overall prioritizing.

The Cybersecurity industry

I compare the cybersecurity industry to the following (admittedly overly simplistic) analogy: You need to build a new house because your old one is falling apart and have a set budget available. You make your way to a home improvement store and tell them you want the most important parts for your house. They tell you about a new water heater feature "you need to have", which they happen to have a relationship with the manufacturer. They explain that it is better than any other water heater, but fail to explain why this special feature (and its added cost) should be part of your house – at the expense of some other feature which you will have to bump off your shopping list.

Confused, you go to the next home improvement store and they tell you they happen to also be the sole manufacturer of a new kind of water treatment system that "you need to have", otherwise you may damage your health from drinking tap water. You are not aware of evidence that there is health damage from tap water in your area, but you've heard stories from elsewhere. It costs so much that you would need to bump the interior paint job off your shopping list. Confused, you move on … everything seems important but you can only buy/do so much.

You hire a consultant to help you build your house, but she/he has vetted manufacturer relationships so you don't trust her/him anymore. In the end, you buy a bunch of stuff based on hearsay about what needs to be done and what doesn't. Back to cybersecurity, many customers can only do a few things. "I only have time to do the top 10– but what are those?!"(or other number than 10, depending on time and budget).In order to figure out what those top 10 are, we as the defender ecosystem need generally accepted structure and metrics.

Why is this hard. Hasn't it been done before?

Unfortunately, like well thought - through answers, the answer to the question what is the exact number and prioritization is often "It depends...". It depends on: What systems? What applications? What data? Scale of IT landscape? Functional aspects? Non - functional aspects? Financial/organizational constraints?...

Why can OWASP, the Open Web Application Security Project (owasp.org), for example, give us a simple top 10 based on concrete metrics, while for general cybersecurity we are stuck with hundreds or thousands of controls? OWASP can do a top 10 because it is mostly covering a specific problem, use - case, and technology (web applications). In the bigger picture of cybersecurity of most organizations, web applications usually are only one aspect of many that need to be dealt with.

The BSI Baseline Protection Manual is another example that illustrates how more specific cybersecurity instructions can be provided for specific networks, system and applications: The BSI standards provides concrete "catalogues" with specific cybersecurity instructions1 for various specific systems and applications. As with OWASP, each covers a specific problem, use-case, and technology. Indirectly related to that are "protection profiles" for various systems based on the ISO/IEC 15408 Common Criteria (commoncriteria.org) standard for computer security certification.

Common criteria gives certifiers more flexibility by allowing them to specify the requirements and the particular IT environment ("Target of Evaluation", ToE). On the flipside, it leads to significant confusion about what requirements and ToE were exactly covered. For example, certifying a login window of product allows the vendor to misleadingly claim their product is "common criteria certified". So if your cybersecurity needs to cover more than the covered point solutions (usually the case for enterprise cybersecurity, where a lot of the intelligence is in the system-of-systems "glue" between systems) – and you cannot go down a high-assurance architecture route either (usually the case for enterprise cybersecurity as well) – then what now?

Numerous generic compliance frameworks, standards and guidance (i.e. not for a specific ToE or use case) have been produced, giving a great broad overview of many things you may consider doing. For example, NIST 800.53 "Security and Privacy Controls for Federal Information Systems and Organizations"2 provides guidance for hundreds of controls across numerous categories ("families):

ID	Family	ID	Family
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Envirmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personal Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Aquisition
IA	Identification and Authentication	SC	System and Communication Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

Some real metrics?

Where can we get some real metrics and statistics? There are definitely some real metrics out there as to what should be done for maximum cybersecurity "bang for buck". For example (just to name one), the Australian Dept. of Defence (ASD) published "The Top 4 Strategies to Mitigate Targeted Cyber Intrusions3", claiming that they established metrics that show that those top 4 prevent 85% of breaches.

Here is the list:

1. Use application whitelisting to help prevent malicious software and unapproved programs from running
2. Patch applications such as Java, PDF viewers, Flash, web browsers and Microsoft Office
3. Patch operating system vulnerabilities
4. Restrict administrative privileges to operating systems and applications based on user duties.

They also published a top 35 list, based on the same metrics, together with its effectiveness score:

Mitigation Strategy Effectiveness Ranking for 2014 (and 2012)		Mitigation Strategy	Overall Security Effectiveness
1	(1)	**Application whitelisting** of permitted/trusted programs, to prevent execution of malicious or unapproved programs including .DLL files, scripts and installers.	Essential
2	(2)	**Patch applications** e.g. Java, PDF viewer, Flash, web browsers and Microsoft Office. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest version of applications.	Essential
3	(3)	**Patch operating system vulnerabilities**. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest suitable operating system version. Avoid Microsoft Windows XP.	Essential
4	(4)	**Restrict administrative privileges** to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.	Essential

Once organisations have effectively implemented the Top 4 mitigation strategies, firstly on workstations of users who are most likely to be targeted by cyber intrusions and then on all workstations and servers, additional mitigation strategi

5	(18)	**User application configuration hardening**, disabling: running Internet-based Java code, untrusted Microsoft Office macros, and unneeded/undesired web browser and PDF viewer features.	Excellent
6	(N/A)	**Automated dynamic analysis** of email and web content run in a sandbox to detect suspicious behaviour including network traffic, new or modified files, or other configuration changes.	Excellent
7	(21)	**Operating system generic exploit mitigation** e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).	Excellent
8	(11)	**Host-based Intrusion Detection/Prevention System** to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence.	Excellent
9	(5)	**Disable local administrator accounts** to prevent network propagation using compromised local administrator credentials that are shared by several workstations.	Excellent
10	(7)	**Network segmentation and segregation** into security zones to protect sensitive information and critical services such as user authentication by the Microsoft Active Directory service.	Excellent
11	(6)	**Multi-factor authentication** especially implemented for remote access, or when the user is about to perform a privileged action or access a sensitive information repository.	Excellent
12	(8)	**Software-based application firewall, blocking incoming network traffic** that is malicious or otherwise unauthorised, and denying network traffic by default.	Excellent
13	(9)	**Software-based application firewall, blocking outgoing network traffic** that is not generated by a whitelisted application, and denying network traffic by default.	Excellent
14	(10)	**Non-persistent virtualised sandboxed trusted operating environment**, hosted outside of the organisation's internal network, for risky activities such as web browsing.	Excellent
15	(12)	**Centralised and time-synchronised logging of successful and failed computer events**, with automated immediate log analysis, storing logs for at least 18 months.	Excellent
16	(13)	**Centralised and time-synchronised logging of allowed and blocked network activity**, with automated immediate log analysis, storing logs for at least 18 months.	Excellent
17	(14)	**Email content filtering**, allowing only whitelisted business related attachment types. Preferably analyse/convert/sanitise hyperlinks, PDF and Microsoft Office attachments.	Excellent
18	(15)	**Web content filtering** of incoming and outgoing traffic, whitelisting allowed types of web content and using behavioural analysis, cloud-based reputation ratings, heuristics and signatures.	Excellent
19	(16)	**Web domain whitelisting for all domains**, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.	Excellent
20	(19)	**Block spoofed emails** using Sender ID or Sender Policy Framework (SPF) to check incoming emails, and a "hard fail" SPF record to help prevent spoofing of your organisation's domain.	Excellent
21	(22)	**Workstation and server configuration management** based on a hardened Standard Operating Environment, disabling unneeded/undesired functionality e.g. IPv6, autorun and LanMan.	Good
22	(25)	**Antivirus software using heuristics and automated Internet-based reputation ratings** to check a program's prevalence and its digital signature's trustworthiness prior to execution.	Good
23	(24)	**Deny direct Internet access from workstations** by using an IPv6-capable firewall to force traffic through a split DNS server, an email server, or an authenticated web proxy server.	Good
24	(23)	**Server application configuration hardening** e.g. databases, web applications, customer relationship management, finance, human resources and other data storage systems.	Good
25	(27)	**Enforce a strong passphrase policy** covering complexity, length, expiry, and avoiding both passphrase reuse and the use of a single dictionary word.	Good
26	(29)	**Removable and portable media control** as part of a Data Loss Prevention strategy, including storage, handling, whitelisting allowed USB devices, encryption and destruction.	Good
27	(28)	**Restrict access to Server Message Block (SMB) and NetBIOS** services running on workstations and on servers where possible.	Good
28	(20)	**User education** e.g. Internet threats and spear phishing socially engineered emails. Avoid: weak passphrases, passphrase reuse, exposing email addresses, unapproved USB devices.	Good
29	(26)	**Workstation inspection of Microsoft Office files** for potentially malicious abnormalities e.g. using the Microsoft Office File Validation or Protected View feature.	Good
30	(25)	**Signature-based antivirus software** that primarily relies on up to date signatures to identify malware. Use gateway and desktop antivirus software from different vendors.	Good
31	(30)	**TLS encryption between email servers** to help prevent legitimate emails being intercepted and used for social engineering. Perform content scanning after email traffic is decrypted.	Good
32	(32)	**Block attempts to access websites by their IP address** instead of by their domain name, e.g. implemented using a web proxy server, to force cyber adversaries to obtain a domain name.	Average
33	(33)	**Network-based Intrusion Detection/Prevention System** using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.	Average
34	(34)	**Gateway blacklisting** to block access to known malicious domains and IP addresses, including dynamic and other domains provided free to anonymous Internet users.	Average
35	(35)	**Capture network traffic** to/from internal critical asset workstations and servers as well as traffic traversing the network perimeter, to perform post-intrusion analysis.	Average

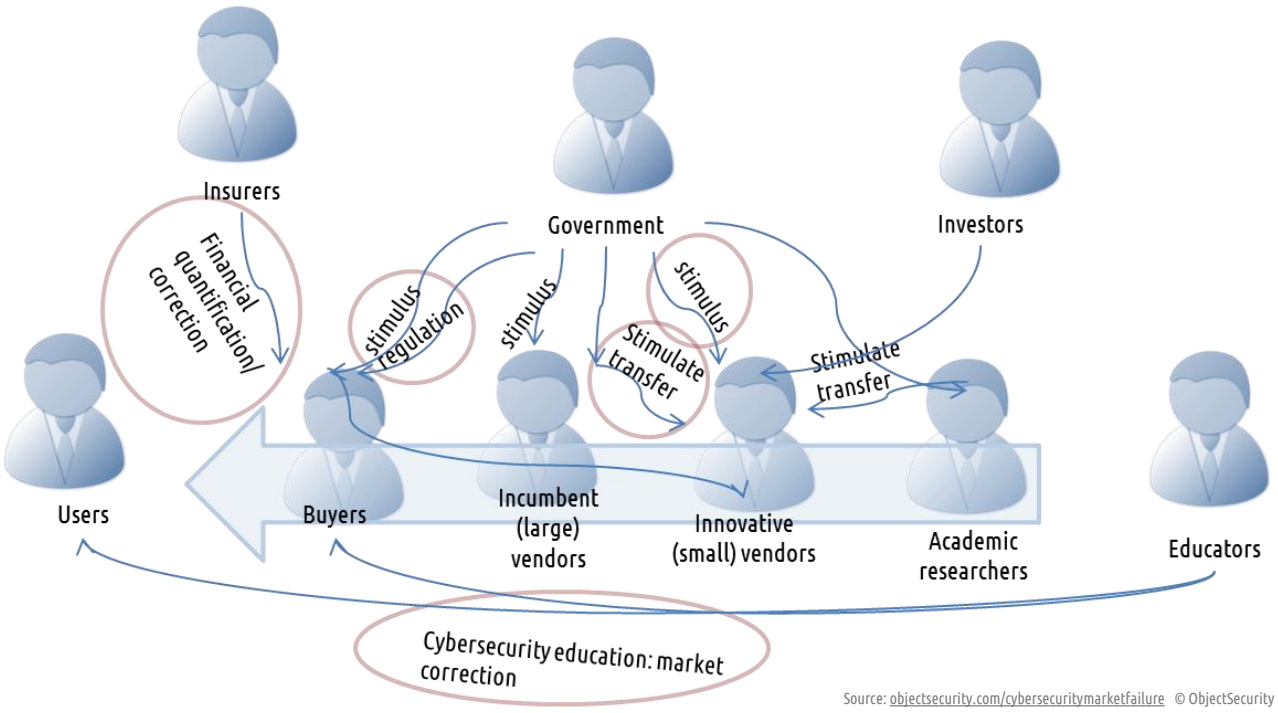
asd.gov.au/publications/protect/top_4_mitigations.htm

You may find that your organization's purchasing decisions differed from the priorities presented here. Or you may disagree altogether that this ranking is even accurate, because many others say many other things.

Let's step back: Cybersecurity market failure…

Let's look at the bigger picture for a moment: Why do we need to even discuss this? Why doesn't the cybersecurity ecosystem fix itself? Why do customers need to figure out the priorities, digging through numerous frameworks and guidance, while at the same time being bombarded by vendor-driven prioritizations? Because cybersecurity is perpetually in what shares many characteristics of a market failure. Market failure is an economic term defined (in a nutshell) as (1) inefficient allocation of goods/services, (2) based on pure self interest, and (3) can be improved from a societal point of view.

Market failures can be caused by "time inconsistent preferences, information asymmetries, non-competitive markets (market power), principal–agent problems, externalities, or public goods" (as an economics concept in general4). Usually, market failures require interventions, for example by self-regulatory organizations, governments or supra-national institutions. Note that market failure does not imply that there is no money in the market – instead it means that the market is inefficient in terms of resources and societal impact. In 2015, ObjectSecurity's Dr. Lang presented a talk about cybersecurity market failure at ISSA Cornerstones of Trust5, outlining the interactions between numerous cybersecurity stakeholders and how they (inadvertently or intentionally) put barriers in place for each other – slowing the progress of the defender ecosystem:



This market failure is part of the reason why the protector ecosystem is progressing too slowly, falling behind the attacker ecosystem. Another reason is that (in simplistic terms) defending is much harder than attacking – defenders need to do it right everywhere all the time (i.e. protect everything), while attackers only need to do it right once (i.e. find one vulnerability).

Cybersecurity adoption roadblocks

As a consequence: On the defender side, few "game-changers" find wide adoption (e.g. attribute-based access control, micro kernels, privacy avatars etc., just to name a few), while the bad guys' ecosystem progresses quite well. In fact in many instances the attacker ecosystem is better aligned than the defender ecosystem.

Relating this back to this whitepaper's topic, the defender ecosystem is a cacophony of vendors, consultants, integrators, agencies, etc., everyone working within the constraints of the overall cybersecurity market failure. As a result, the defender ecosystem has not been able to effectively come together to provide a generally accepted, metrics-based ranking of cybersecurity activities. This leaves the task of figuring out what to do to customers, basing decisions on the daily cacophony of vendors, consultants, integrators, governments, media, etc.

So what should you do?

It is not the primary purpose of this whitepaper to postulate a top 10 list, but rather to discuss the needs and challenges to get to industry-wide vetted metrics of what matters most in cybersecurity (potentially with some adaptations based on industry, IT landscape, regulatory/legal environment etc.) The primary purpose of this whitepaper is to nudge the cybersecurity industry in a direction where customers can decide based on clear metrics where they should put their priorities, rather than leaving customers in the current state of confusion caused by the noise created by the cybersecurity industry.
Let's look at typical intrusion patterns to potentially guide us.

Intrusion phases can be categorized into six phases6: Reconnaissance; Initial Exploitation; Establish Persistence; Install Tools Move Laterally; Collect; and Exfiltrate & Exploit. Attacks often start with finding holes in less-protected systems, or tricking users into doing something to open up a hole. The attacker may try to get such a foothold in uncritical devices because they are usually less protected. There may be nothing to do/steal there, but it usually allows the attacker to move on laterally ("pivot") to more critical assets, eventually getting access to valuable resources. It is important to distinguish the phases and appreciate how these phases are connected to determine the countermeasures that need to put in place. For example:

Countering initial exploitation

It is important to prevent as much in the early stages (initial exploitation) as possible, e.g. by using antivirus tools, email attachment scanners, good authentication etc. However, at the current state of the cybersecurity ecosystem you need to assume that these countermeasures will fail at some point (e.g. "zero-day malware" which your antivirus tool doesn't know yet). It could be that unsecured "smart" lightbulb that may be the starting point for the hacker. In fact seemingly uncritical IoT devices are currently a major source of vulnerabilities (and have been used by hackers to cause a major internet outage in November 2016).

Another major source of attacks is that some user in their organization will eventually click on a (spear-) phishing email attachment or website link – people are processing so much information every day that human errors are to be expected (even if only due to freak event circumstances such a names matching colleagues etc.), even for security-educated individuals. And sufficiently locking down email attachments or websites is not really feasible for most organizations either because that would reduce productivity. So you have to assume that some initial exploitation will happen eventually.

Countering pivoting (lateral movement)

Therefore, in addition, you need to minimize the impact ofsuch successful exploitations. A great way to do this is by implementing more fine-grained access controls across your networks, systems, devices and applications. Instead of giving particular users or devices broad access to much information and many systems, devices, and applications, you need to reduce access to the "minimum needed" to get the task done.

This will likely involve contextual, dynamic, fine-grained access control technologies (for example "attribute-based access control", ABAC7). This is contrary to the traditional "hard shell, soft inside" security model where firewalls are put in place to control who can get in and out of an enterprise network. With "bring your own device" (BYOD) and cloud computing rapidly used by organizations today, traditional trust boundaries are messy or non-existent, making "hard shell, soft inside" ineffective.

Knowing when it happens & impact control

Security is never 100% .So assuming that both those and everything else you put in place fail, you need to have tools (and people!) in place who can detect that you got breached. In addition, you need to figure out ways of how your organization will recover from a catastrophic hacker/failure event. Just to name a few examples, mirror sites, hot/cold backups etc. are necessary, as well a way to restore systems to a clean state after being attacked.

So how do you prioritize? Without clear metrics it is hard to estimate how likely which kind of vulnerability and associated impact will be.

Why don't we (the defenders) share all metrics?

There are a number of sources that provide some good metrics about cybersecurity vulnerabilities (search for "cybersecurity breach reports" on the internet). Most are related to antivirus and web applications. Broader cybersecurity breach metrics are much harder to find, mostly because organizations are reluctant to share details after breaches about how they were breached. This lack of sufficient data makes it hard to consolidate reliable metrics (needed to determine a solid ranking of what needs to be done). Governments and industry organizations are working towards sharing cybersecurity incident information, but not nearly enough. Without a comprehensive information sharing initiative across all stakeholders, we are likely to not get reliable-enough, generally accepted cybersecurity metrics. Instead we need to dig through the "cacophony" and try to guess metrics ourselves – clearly neither effective nor efficient.

How much time and money do you have?

Time and money (and also cybersecurity competency) limit how much you can do. Cybersecurity teams are often overworked, understaffed, fire-fighting breaches etc. These limitations determine how far down the list of "to-do's" you can realistically ever get.

How do we make pivoting harder for enterprise IT landscapes?

There is a lot of talk across the cybersecurity industry around reducing attack vectors related to initial exploitation (antivirus etc.), and related to knowing when you got breached (incl. continuous monitoring, intrusion detection, log analysis etc.) What is much less talked-about is how to make pivoting harder for enterprise IT landscapes – access controls are the main mechanisms to limit the options for pivoting.

However, today access controls are typically not effective enough: too coarse-grained, not adaptive/contextual enough, and not enforced at enough points in enterprise IT landscapes. Moving the needle to get to more effective access controls usually makes access control too hard to manage and implement. Attribute-based access control (ABAC) has often suffered from this challenge – while technically enabling better access control, it also makes access control much harder to implement. Easy and effective are seemingly at odds when it comes to enterprise access control.

Fortunately there are tools such as for example ObjectSecurity OpenPMF that bring those "odds" together, enabling powerful security policy implementation that's also effortless to manage. This simplification is achieved by allowing users to author rich access policies in generic terms, and automatically filling in the technical details for a concrete technical security policy implementation (e.g. attribute-based access control) automatically by detecting and analyzing information about you organization, its users, and it's networks, systems and applications (click here for a whitepaper about OpenPMF 4.0).

This is just an example of what appears to be a strong priority, but is often not ranked high enough to even get done. And why would you know if you should believe my opinions voiced in this whitepaper anyway? How should customers determine whether this (as an example) really matters, and whether it matters more than something else they are doing or planning to do? Unfortunately, currently customers are left in the dark, because as said above there are no widely-accepted good metrics-based rankings that would tell you that this is more or less important than something else.

Some final thoughts…

It should be helpful to at least broadly structure major priorities based on a thought process. In particular, there are ongoing discussions in the cybersecurity industry about whether – and in which order of priority –you should:

- **Prevent:**
  One school of thought makes preventing breaches by reducing attack surface and vulnerabilities the "plan A". This approach is usually followed by more mission-critical/safety-critical industries and military/intelligence.
- **Detect & respond:**
  Another school of thought around cybersecurity professionals is that prevention is relatively futile, and you should rather make your efforts on detection and response your "plan A".
- **Control impact (recovery):**
  Yet another (more extreme) school of thought thinks that both prevention and detection are quite futile, and we should mainly focus on impact control and recovery.
- **Sell it to management and auditors:**
  And yet another school of thought thinks that the primary objective is to convince management auditors that security meets (compliance) requirements.

The author's (personal) view is that prevention should still be "Plan A", followed by "detect & respond, followed by impact control, and lastly sell it to management. But this is open to debate until we have more solid, generally accepted industry-wide metrics…

The Top 10

But in case you have been waiting for a "Top 10" list, here is my personal current top 10 list based on that rough prioritization, followed by a short appendix with further details:

Top 10		
Protect + Detect + Respond + Impact Control + Recover + Value	1	Identify your critical assets and focus on those – trust boundaries
	2	Improve authentication: 2factor, biometric
	3	Improve access control: ABAC, whitelisting, policy automation, least privilege esp. for admins
	4	Patch apps/OS etc. (fast turnaround!)
	5	Build security in (isolate): VLANs, fine-grained access
	6	Encrypt critical data
	7	Test security & fix
	8	Monitor, but close the loop between detect & enforce
	9	Backups, and plan for recovery from worst case scenario
	10	Make sure security is seen as an enabler & value

The Top 10, details.

Plan A – Protect

Improve authentication - two-factor, biometric

Improve access control

- Role-based access control necessary but not sufficient.
- Need for something closer to "least privilege" (for admins, but also for M2M/IoT etc.)
- Attribute-based access control (ABAC)
- Policy automation to make ABAC and other access policies manageable

Build it into the architecture & software (if you can): Isolate

- Assume the hacker is in – isolation will make pivoting harder
- Bound your problem space
- Isolate assets, use VLANs etc. (even down to application/process isolation -> SELinux)
- fine-grained attribute-based access control between those components
- Isolate data of different value

Encrypt critical data – maybe by a different stakeholder?

Test your policies, apps, APIs, OSs, VMs, code, backups, whatever!

- Lots of tools, this is the cheap part to find lots of holes to fix.
- However, you don't know what you don't know.
- Fix the stuff that comes up as broken!

Patch!!!

Plan B - Detect & Respond

You will get hacked.

- Either your plan A will prevent the pivot
- Or you can try to be fast
- However: roundtrip from IDS to human to enforcement is often too late (Target hack, anyone …?)
- Tools don't really close the loop because blocking something is dangerous

Close the loop with at least some automation - human in the loop not viable

Move beyond signature/behavior-based detection to policy-based (actually the combination of all of them)

Have admins sit around 24/7…viable? Do they have visibility, and the tools to respond?
The daily firewall update?!

Plan C - Impact control & recovery

Assume that things will go wrong anyway

Backups: in a way that cannot easily be infiltrated (off-site/off-line etc.). Test your backups!

Plan for recovery from total failure of everything…worst case scenario (testing this may be too expensive…)

Plan D - Value & Money

Make sure the money for security keeps coming from management.

- Show value…
- Security as an enabler for business
- Educate
- Help meet compliance

Most of what I see is a security $$$ problem: lack of the right people (staff not incentivized enough), lack of budget or budget spent totally wrong, results are accordingly…

About the Author

Dr Ulrich Lang: Ulrich Lang is ObjectSecurity's founder & CEO; Ph.D. from University of Cambridge Computer Laboratory (Security Group) on access policies; Master's Degree (M. Sc.) in Information Security from Royal Holloway College (London) in 1997. Ulrich is a renowned thought leader in access control policy, model-driven security, and Cloud/SOA/middleware security, identity & access management.

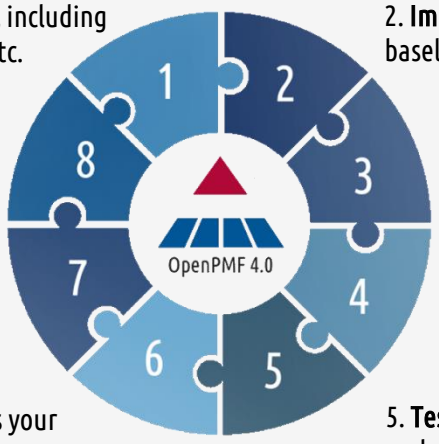
He is on the Board of Directors of the Cloud Security Alliance (Silicon Valley Chapter). He is co-inventor and co-developer of ObjectSecurity's OpenPMF product. He delivers some of the professional services ObjectSecurity offers He has published over 150 papers/presentations, and has previously worked as a proposal evaluator, project evaluator, conference program committee, panel moderator, consultant, book author, technical expert witness.

About ObjectSecurity® and OpenPMF Security Policy Management

OpenPMF™ Makes Security Policy Manageable Through Automation. ObjectSecurity's OpenPMF security policy management platform stops security breaches with powerful policy enforcement. It gives you powerful security policy implementation that is also effortless to manage. It allows you to improve protection, monitoring, testing, and documenting – for your information, users and devices. OpenPMF™ turns human-manageable security policies automatically into the matching preventive technical implementation. OpenPMF lets you manage security policies in customizable terms that matter to your organization. OpenPMF ensures policies are manageable even if IT landscapes are large and change dynamically. The result is a significant cost saving, esp. with respect to maintenance.

1. **Import information** about your organization, including systems/applications, data flows, users, alerts etc.

2. **Import** your existing technical **policies** as a baseline, for example access control configs



3. **Author** security policies that are intuitive, generic, rich, customizable

4. **Generate** technical enforcement rules & configurations, for example access control

5. **Test** using formal model checker methods, and **document** for audit & compliance

6. **Enforce** consistent "defense in depth" across your IT via **OpenPMF's enforcement** and **3rd party exporters**

7. **Monitor** policy enforcement alerts centrally to help policy management & remediation

8. **Update** technical enforcement automatically if your IT changes and **customize** OpenPMF