White Paper

The 'Security' Paradox

A more sensible look at information protection

Intended audience: Those who want effective protection.

Part .1. Problem:
Why information technology related 'security' fails to deliver.
Status: RFC
Publication: 2nd Quarter, 2012

Part .2. Solution:
How much easier and more cost effective 'information protection' can be.
Status: Draft, needs to be finalised.
Expected: 4th Quarter, 2012
**Part .1.**

**Executive summary:**
At present popular 'security' is largely based on costly stubborn misconceptions and conflict of interests. In this first part we explain in layman's terms what is really causing the widespread 'security' failure. This takes a bit of effort to read through, but will be worthwhile. This document will enable you a better grip on information protection concerns, by providing insight into the major factors for failures in the mainstream 'security' approach.

In part 2, we explain in layman's terms how to move from this conventional mainstream 'security' towards practical 'information protection' with clear logic and sensible structure. To give you some idea of what it takes to get it done.

This innovative protection methodology does of course not provide the mythical 100% 'security' , but should increase the protection level dramatically. The factual 'In Control' status can now be achieved. At the same time it can bring about significant reduction in costs by eliminating issues like counter productive complexity. Also there will be other beneficial effects like naturally increasing overall skill level, adaptability and job satisfaction.

In order to achieve all this we would teach and guide you and your people. So you can incorporate it into your organisation without lasting dependencies on external advisers. Usually on a balance we don't cost money, but we actually save you a significant amount of money. Moreover, we dare stand for the results we achieve, as far as giving you a money-back guarantee. So we're not just cost-saving investment, we're also a risk-free one. That makes us rather unique.

**Introduction:**
Today most organisations are dependent on the information flows handled by computer systems. Protecting those information flows is therefore crucial, but almost all organisations fail to do so effectively. Just a small alteration of a public facing web-site can put the reputation at stake. A severe disruption of the main systems, which only takes a few seconds, can take days to recover from while putting the whole organisation at a complete standstill during that time. Specially now 'hacking' has become rather popular also amongst governments and rival companies.

On the other side of the spectrum, research shows that international banks are only compliant on paper with the relevant information protection laws and regulations — in reality are not even close to it, thus breaking the law.

Organisations whose primary focus is 'security' — like secret service agencies, academic research groups and well known companies — seem to neglect the basic protection principles. Information Technology and Security people tend to use the standard cop-out "but we can't secure it 100%" to justify continuing as before and wasting budget on yet more expensive products and procedures, instead of dealing with what ever is actually causing that structural failure.

So... the "But why!?" question arose, and a long term research project came to life. The project has reached its goal in 2011. This dual white paper is a result of a decade of completely independent field research by QCIC.nl members, involving a wide variety of organisations around the globe.
Different cultures have different habits, but since all regions seem to follow the international 'main stream' when it comes to office culture, the observations seem to apply across the board. The following pages describe the interconnected factors which are causing that structural failure:

**Root cause**
1. Complexity overload
2. State of denial
3. Retreating into blind faith

**Attitude**
4. King of the hill syndrome
5. King of the castle
6. Macho IT culture

**Employ**
7. Hiring process is inherently self-destructive
8. Unqualified to qualify
9. Pleasant colleagues, may be the wrong choice

**Mind the gap**
10. Blocking top-down structure
11. Academic reality bending, mind the gap
12. The Standards deception
13. Certification mono-culture
14. Over simplification, also known as: The 3 robot laws
15. Conflict of interests, used car salesman methods
16. Outsourced, doesn’t mean: don't worry
17. Nerds make nerd toys, not good products
18. Gap between hardware and software makers
19. Skipping the basics, to play with exciting toys

**Thinking outside the box**
20. Losing sight of the weakest link
21. Asking 'hackers' to do 'security'
22. Stubborn misconceptions

During the process we fortunately also found effective solutions which turn out to fit nicely into one clear methodology. [once you know how, it is simple!]

The majority of the verification testing has been done discretely, within different types of operational structures, in order to minimise change resistance from those involved. Some of those organisations have now fully implemented the 'Advanced Self Correcting Structure', others still cling to their old habits and unfortunately don't dare to commit to walking one step ahead of the mainstream.
Approach to analysis:

Standard Root Cause Analysis is a bureaucratic management driven process. It identifies some things as 'the root cause' the very moment it suits those who are conducting the investigation. The resulting outcomes of such narrow path RCA projects are inherently a few layers above the actual root cause of the problem. So they will then try to action corrective measures for something which is best described as 'sub-layer symptoms' instead of dealing with the actual 'root cause'.

We have created 'absolute root cause analysis', which digs down to the actual bare bones of a problem. With this more sophisticated approach, the label 'root cause' is only used when it satisfies the curiosity of the extremely repetitive 'but why !?' question for 3 objective viewing angles. Those angles are: logical, structural and motive.

Before continuing reading, one needs to be aware of a very fundamental brain mechanism which is called 'self-justification'.

A brain will by default automatically first try to dismiss evidence if it contradicts the fundamental belief structure. Secondly the brain's 'security' mechanisms create a feeling of anger from frustration, if it can not easily dismiss such bothersome new information. That feeling of anger can than be used as a convenient excuse to justify the dismissal of the whole subject, in order to continue as if the unpleasant evidence never existed.

Let's set the pace by stating that: 'Security' is a mythological beast. The word itself creates false expectations with severe consequences. To get a clean foundation to build on, one needs to eliminate that underestimated beast.

"Protection is preparation, Security is a mere desire "  
Protection: from pro- ‘in front’ + tegere ‘to cover’  
Security: from se- ‘without’ + cura ‘care’
What is causing the structural failure:

1 ~ Complexity overload
The root cause of many of the following issues can be found in a neural overload defence mechanism.
A person doing a job is supposed to be 'in control' of the tasks that come with it. But with the extremely over complex structures which have become the standard these days, it is no longer possible to comprehend it all. If the mind is not trained to deal with such dynamic complexity (there is no mainstream educational institute which teaches this rather useful skill), the brain gets into a state where automatic reactions start hampering the healthy functioning of the person. Consequence is a significant amount of blocking-out more input in order to prevent physical discomfort from brain overload.

Occurrence: Common
Detection: 1 test question
Solution: #S-01
Cost: Insignificant
Effort: Little

2 ~ State of denial
A side effect of the overload issue is often a state of denial about the inability to be in control. When a person in such a mindset is confronted with the fact that they are not in control they can go to extreme length to try and camouflage that fact. A classic response is repeating "That is just an opinion!", when inescapable proof is presented.

[Children can stop paying attention and go play with sand / Most adults are under social pressure to act like they can keep up all the time]

Occurrence: Common
Detection: 1 test question
Solution: #S-02
Cost: Insignificant
Effort: Some

3 ~ Retreating into blind faith
Many just pick a popular 'solution', without too much thought about whether it is a decent option for their specific situation. If one generally feels not able to deal with the overload of options, an easy way out seems to just follow majorities and hope things will be fine. And if not..., at least one can take some comfort from having resorted to 'standards' (*)

Where some are aware of this capitulation and are prepared to suffer the consequences. Others (usually the larger organisations) aren't and merge into a very particular state of denial: one in which they confuse their rather random choice as 'the only option'. Followed by putting immense effort & resources into trying to control all which was supposed to reduce effort. Instead of just taking an hour or two to learn how to cut through overload.

Occurrence: Common
Detection: 1 test question
Solution: #S-01
Cost: Reduction
Effort: Little
4 ~ **King of the hill syndrome**
A person who doesn't feel in control of the job, will often go to great length to keep out any form of criticism/competition.
One of the consequences of this is that they will try to make sure that only even less qualified people will be hired, so the overall situation will become gradually worse.

Occurrence: Common  
Detection: Easy  
Solution: #S-03  
Cost: Insignificant  
Effort: Normally the nifty trick described in #S-02S can be used to get a person out of that mindset. 
But success depends on age and stubbornness. 
Otherwise leaderships willingness to remove influence power from the person, if too deeply locked into such a state.

5 ~ **King of the castle**
A person who owns, or manages part of, an organisation and feels too authoritative, can start making up arbitrary rules without checking if they are realistic. This often is combined with not tolerating any criticism. The situation is created by the same complexity overload issue in combination with a power trip.
The consequence is that people working for the 'King of the castle' must do things which they know are counter-productive in order to keep their job. Most often they will focus on making everything look good on paper and ignore/hide the actual state as long as possible.

Occurrence: Common  
Detection: With a trick question.  
But should **not** be exposed, because that only makes a King retreat into aggressive denial.  
Solution: #S-04  
Cost: Little  
Effort: Some

6 ~ **Macho IT culture**
It is no secret that the Information Technology playground has a macho culture for both men and woman.
One of the consequences is that a problem is normally not tackled with the most pragmatic solution, but an opportunity to show off with the most fancy 'solution'. Resulting over time in an over-complex mess, and triggering the King of the hill syndrome and other unpleasant side effects.

Occurrence: The norm  
Detection: Takes a minute from outside, by merely looking at the IT structure.  
Solution: #S-05  
Cost: Reduction  
Effort: Minimal
7 ~ Hiring process is inherently self-destructive
The standard hiring process is from a time when the archive was still a room full of paper maintained by office clerks, instead of the current digital one maintained by technicians. The personnel department has distanced itself from their co-workers and now calls itself 'HRM' (Human Resource Management) but other than that has not kept up with the change into the digital era. They still use the same old selection method, which is not suited for getting the proper technical people but instead still favour the bureaucratic office clerk type.

Occurrence: The norm
Detection: Easy
Solution: #S-04
Cost: Reduction
Effort: Some

8 ~ Unqualified to qualify
Another issue is that HRM people who do the CV screenings don't understand technical CV's, so they just try to match keywords and acronyms. Which means that they automagically weed out the more qualified people and then present the 'good match' barely qualified CV's to a department chief who is doing the final selection.

A typical example: (no need to understand those acronyms)
The IT department chief asked, "Requirements: CISSP, academic degree, experience with AIX."
John's resume states: "10 years as security consultant for Banks, Certified Senior Unix Engineer, Polytechnic microelectronics diploma."
Pete's resume states: "Masters degree in computer science in 2010, CISSP, AIX v4.2"
The HRM department will put John's resume in the rubbish bin without hesitation, and proudly show Pete's to the IT department chief.
The IT department chief, made blind by the meddling HRM department, will have to pick Pete as their new engineer, a guy who has briefly worked with an AIX version from over 10 years ago at the university judging from the version number and doesn't have decent practical knowledge to do the job, but on paper seems the perfect match.

The consequence is that organisations which use such HRM or outsourced screening, generally get stuck with the “if you can't make it, fake it!” type of, incompetent 'specialists'. Which triggers the King of the hill syndrome right from the start of their new job.

Occurrence: Sadly, the example doesn't show an exception but the norm.
Detection: Easy
Solution: #S-03 + #S-05
Cost: Reduction
Effort: Minor

9 ~ Pleasant colleagues, may be the wrong choice
Normally people who are looking for someone to strengthen their organisation will make “pleasant colleague for the team” one of the prime selection criteria.
The drawbacks of that thoughtless but understandable choice are:
- Will exclude any healthy counterweight perspectives.
- Will exclude the ‘tough cop’ type, which is crucial for the 'security officer' position.
- Will create an inherently fragile mono-culture.
- Will create an inflexible organisation.
- Will create an introverted and disconnected organisation.
- Will make an organisation conservative, so not able to keep up.
The consequence is that most organisations can't handle exceptions and dismiss justified criticism from outside. So they fail to deal with the reality of the fast changing world, and are genuinely surprised every time their name appears in the news media when they have another crisis.

Occurrence: The norm
Detection: Clearly visible on the outside
Solution: #S-05
Cost: Reduction
Effort: Insignificant
10 ~ **Blocking top-down structure**
Most organisations are hierarchical and strictly divided into departments.
Many pretend or want to be open minded, but when tested, the upper layer turns out not as approachable as they like to proclaim.
The consequence is that there is a social iron curtain preventing crucial information from moving up the ladder to those who need to act upon it. Creating a detached management layer which is unaware of what is going wrong, until it has developed into a crippling issue so blatant that it is noticed by either management or the news media.

Occurrence: The norm
Detection: Easy
Solution: #S-06 + #S-01
Cost: Insignificant
Effort: Minimal *(no change needed to the existing organisational structure!)*

11 ~ **Academic reality bending, mind the gap**
People with a university degree have learned to think based on isolated lab situations and the theory that fits it. According to the Professors *[King of the castle]*, universities are focused on isolated theoretical knowledge, not on teaching students practical job skills. It is well known that there is a significant gap between the theory based academic world view and the far more kinetic and organic operational situations.

People with such a background often *try to force* reality to fit their abstract models, instead of adapting to the actual situation. Which creates rather surreal work environments where, for example, a person with a university degree tells an experienced, but lower in the hierarchy, field engineer that things have to be done rather differently, while the engineer knows that that will not turn out good, but has to do it anyway. The field engineer normally can’t just prove the disconnected academic theory wrong with academic argument, and even if that field engineer can, the academic would not know what to do next. So valid arguments like "I know from experience" or "See for your self" will conveniently be discarded. *[self-justification]*
The consequence is that security architectures and products made up by people with such a background normally only look good on paper, but make really experienced specialist shake their heads in disbelief.

Occurrence: Very common
Detection: A little effort
Solution: #S-02 + #S-03L + #S-05
Cost: Depends on how deeply rooted
Effort: " "

12 ~ **The Standards deception**
A two part issue.

**Part 1:** Organisations normally opt for adopting a standard, instead of just becoming compliant.
So, instead of *only* changing what *needs* to be changed, they just start doing it all exactly as described in the standard. This is done because it seems easier, but it can transform an organisation into something it did not intend to be like. It also creates a mono-culture, taking away the uniqueness and diversity, which is gratefully abused by nosy crackers and industrial espionage.

Part 2: The few currently used official standards have a few inherent drawbacks:
1. By default outdated. It takes office years to create and adapt a standard way of working.
2. Mostly come from dusty laboratory theory, rather then grown from field experience.
3. By their very nature impose a conservative structure and thus restrict progress.
4. Are too bulky and at some points incoherent.
5. *[restricted information]*
6. The accompanying procedures for the work-floor are commonly over simplified which removes the needed flexibility to handle out of the ordinary situations.
7. Are generally made for foreseen events, thus fail to deal with many major threats.

Occurrence: The norm
Detection: Advertised by the organisation
Solution: #S-07 + #S-01
Cost: Depends on how deeply already rooted
Effort: " "

© adw@QCIC.nl
13 ~ **Certification mono-culture**
When organisations only use people who are committed to *one* dogma, they expose themselves to predictable failure. Plus there are many major shortcomings in the ISACA/(ICS)/ISO doctrine.

**Occurrence:** The norm  
**Detection:** Easy, check for standard fundamental mistakes made by those who trust upon the doctrine.  
**Solution:** #S-01 + #S-05  
**Cost:** Insignificant  
**Effort:** Reasonable

14 ~ **Over simplification, also known as: The 3 robot laws**
Policies are translated into work procedures. Work procedures are then often made obligatory, so deviating from *The Procedures* is not an encouraged option. Translating policies into procedures is usually achieved by writing down what is normally done to get the desired result. This is a narrow-path approach which doesn't take exceptions or change into account. Another issue is that procedures are normally written in a so called 'idiot prove' form, so in theory any co-worker should be able to follow such a procedure to get the same result. The resulting over-simplification creates a volatile catch-22 situation when an exception pops up. The person who has to deal with that situation is bound by the procedures which do not provide a solution, and is not allowed to deviate from the written instructions.

A common situation: Someone behind a counter tells you that something which is perfectly reasonable, is *not possible*! When you both know that it *is possible*, if they would just act outside the restrictive procedures. Like simply asking their supervisor to take over for one moment.

**Occurrence:** Common  
**Detection:** A test case  
**Solution:** #S-01 + #S-06  
**Cost:** Cost reduction  
**Effort:** Some

15 ~ **Conflict of interests, used car salesman methods**
In recent years it has become *normal* for companies to create half baked products. In order to sell more of them when they break outside the calculated warranty. To keep the customers buying slightly better versions time and time again. Or to sell 'extra' features and information in order to 'help' the customer deal with the product.

Just three infamous examples to make a point: The 'built-in breakdown' in some printers. The locked out features in i-products and the overly complicated database systems.

- Some printers, shortly after the warranty period, suddenly seem to be broken and no longer respond. The company tells people who want to get it fixed that it is cheaper to buy a new one. But someone found out that by holding a specific button combination while turning on the power the 'built-in breakdown' function is reset and the printer works just fine again.
- Some companies like to disable functionality in their products, and enable them in a following New! version. So people are enticed to toss away their just one or two year old expensive product and buy the latest (and soon also the be outdated) version.
- A company that started out with a database product, likes to not only sell software but also expensive consultancy to go with it, to get and keep it actually running. There are products made by other vendors which simply do what is needed without all the bothersome extra complexity and unused functionality.

Those are rather obvious examples of incapacitating products which find their way into your organisation. There are also various less obvious forms of trickery hidden in not only many products but also some certifications and training programs.

**Occurrence:** Becoming more common  
**Detection:** Have someone with know-how scrutinise the offered products and solutions  
**Solution:** #S-05  
**Cost:** Reduction in expenditure  
**Effort:** Depends on how clever the know-how is
16 ~ **Outsourced, doesn't mean: don't worry**

One self-induced misconception is that delegated responsibility can be achieved by merely outsourcing parts of the information flow.

The consequence is that when such an outsourced 'service' gets hacked or fails, the organisation suffers the pain but the service provider merely points at the disclaimer part of the service delivery contract.

**Typical example:** Main website is hosted by a run-of-the-mill service provider and gets 'defaced' on a rainy day. The service provider will argue that they could not have prevented it. The people from the organisation whose public image got seriously damaged can only count their losses and may consider changing to another provider – with all the same risks.

This example could have been prevented by either choosing an extraordinary service provider which does know how to prevent such defacing attempts, or by having your own people take care of the rather fragile image façade. If needed have your IT people (re-)educated on *pragmatic* information protection methods.

- **Occurrence:** Common
- **Detection:** Easy, from outside
- **Solution:** Correct information
- **Cost:** Slight increase
- **Effort:** Depends on the choice

17 ~ **Nerds make nerd toys, not good products**

Technology nerds inherently tend to lose themselves in their own realm. They have little interest in how user friendly their creations really are.

The consequence is that most products are not so user friendly, or are overly complex and bloated with hidden/unused functionality, unstable or unfinished, dysfunctional, and after more than 30 years of 'progress' they still just throw a useless "unexpected error!" at the baffled user every now and then.

This also means that basically all normal security products are by default filled with many kinds of exploitable shortcomings waiting to be discovered.

- **Occurrence:** The norm
- **Detection:** Depends on the type of (both open- & closed-source) product.
- **Solution:** #S-05, for mitigation.
- **Cost:** Depends
- **Effort:** Depends

18 ~ **Gap between hardware and software makers**

Most hardware devices with microelectronic components now contain some software handling. It turns out that software programmers are a rather different type of person from hardware development engineers. People who do both normally have one of those skills predominant, because the different skills need an elementary different type of thought process and also a different knowledge base.

This difference in personality wouldn't be an issue if they were both able to appreciate the difference and work well together on projects requiring both skills. Consequence is that such products normally have a noticeable gap between the hardware and software sections, which can be exploited without either section being able to raise an alarm. There are many recent examples where extremely expensive security devices can be bypassed with a clever trick targeted at that gap. For example the **Trusted Platform Module**, MiFare and various biometric security devices.

- **Occurrence:** The norm
- **Detection:** Needs skill
- **Solution:** #S03L + #S-05, for mitigation
- **Cost:** Depends on number of programmers & engineers and their age
- **Effort:** Significant, but also makes their work more enjoyable
19 ~ Skipping the basics, to play with exciting toys
Most people prefer to use fashionable fancy looking systems.
The expressions "Can't stop progress!" is often used as a quick excuse to justify it, without even checking if it's merely hype without actual progress. There are heaps of such exciting gadgets which are eagerly adopted, but many turn out to create more problems than one can justify as acceptable. With more and more of such gimmicks quickly stacking up over the recent years, overall degeneration has become a factor.

Occurrence: Very common
Detection: 1 minute from outside
Solution: #S-05
Cost: Reduction in expenditure
Effort: Minimal

20 ~ Losing sight of the weakest link.
The weakest link principle is one of the factors for effective information protection. Since the complete chain overview is normally missing, such weakest link is no longer clearly visible. In addition, the chains have become so long that just the large number of links itself is creating a weak structure. One can no longer identify the weakest link by just looking at each individual link, because they differ so much in structure that people with rather different backgrounds would need to look at them, and that again would eliminate the critical overall overview to classify them correctly.
The consequence is that different people get blamed each time one or more links are broken by an intruder or accidental event. Such blaming is counter-productive and unfairly shifts the blame from those responsible for the failing overall structure to the individual participants who can't do much to prevent it from happening again. Thus frustration levels go up and overall quality goes down.

Occurrence: The norm
Detection: Relatively easy
Solution: #S-08, by reducing the significance of the weakest link factor in the overall structure.
Cost: Reduction
Effort: Minimal
+
Long term.
Solution: #S-01
Cost: ±1.5 FTE
Effort: Reducing over time to ±0.2 FTE

21 ~ Asking 'hackers' to do 'security'
To check if it is true that 'hackers' are better at setting up good protection, as the news media likes to suggest from time to time. We did a survey of 20 such prominent hackers who also offer security consultancy. We looked at their website and email protection. When asked why their own systems are just as poorly protected as those of their hacking targets, they responded with the similar excuses [quotes]. Which seems logical, because their focus is on exploiting the weakest links, not on creating a solid protection structure.

22 ~ Stubborn misconceptions
In this white paper we describe the most significant of the elementary misconceptions, fundamental flaws in applied logic and popular myths in the mainstream 'Security' doctrine. The rest needs more than a few lines to be put within the context they are found and the impact they radiate out into the overall structure.
**Conclusion:**

To get decent information protection, the focus must shift from simply adding more and more technology and bureaucracy to a smarter “keep it simple” human work environment. After all, computers were created to make our work easier not more complex, odd and restricted as is the case with the mainstream now.

You may have noticed that many sections not only apply to Information and Communications Technology, but also other areas like physical boundary protection, healthcare and general organisational structures. The solutions provided in part 2. largely also apply to those areas, but are not our main focus at this moment in time.

Change takes time when opposed, so raising awareness about the issues seems a good way to set things in motion.
Addendum:

The following quotes popped up during the past years of research. These are from those who promote (variations of) the mainstream. It might illustrate the structural weakness of it.

[The identity of individuals has been somewhat obscured, because although statements have to be verifiable, no one should be singled out for their beliefs.]

L. Research Coordinator (ISACA.org)
"To remain in compliance, a CISA must just report CPE and pay the maintenance fee."

(ISC)²
"For your CISSP credential, your professional experience has to be in two or more of these 10 (ISC)² CISSP domains."

"When it comes to educating and certifying information security professionals throughout their careers, (ISC)² is acknowledged as the global, not-for-profit leader."
"What’s more, as a member of (ISC)² you’re automatically eligible for deep discounts on valuable information, security textbooks, conference sessions, educational materials, and industry publications."
"Moreover, being certified makes a statement about who you are. You’ll be recognized as a knowledgeable, serious, dedicated professional."

SANS
"In order to stay certified you must demonstrate ongoing competency in the Information Assurance field. There are a variety of options for accomplishing this goal."

Prof. U., Executive Director of the European Network and Information Security Agency.
"ENISA is the EU’s response to cyber security issues of the European Union. As such, it is the ‘pace-setter’ for Information Security in Europe, and a centre of expertise."
"But if, as most analyst reports claim, the human component of any information security framework is the weakest link, then only a significant change in user perception or organisational culture can really reduce the number of information security breaches."
"ENISA, based on our studies, has proposed a series of recommendations to different categories of stakeholders: Providers might consider to Continuously strive for improvement in particular resilience related areas. Operators: should put efforts in further developing and distributing measurements, targets, and best practices in resiliency performance and management."
"Further research to specific areas is recommended."

Professor J.
"Sure, there are a number of important topics that we do not have in our study curriculum. (I am part of a EU project on CIP.). Our IT Security master programme is a result of many compromises (fighting for space in the programme against colleagues with pet projects of their own). I am afraid that this does not sound optimistic."

Dr. D. & prof. dr. P. (Distributed and Embedded Security Research Group)
"research is not driven by business factors, therefore researchers focused on topics that are challenging."
"Some ideas are easier to ‘port’ into the real world, where the assumptions one uses in his/her research do not always hold."

K. Department Manager Automation Networks [CIP development]
"We are not talking about ABB infrastructure. What we talk about is the deliveries to US critical infrastructure and fulfilling the cyber security requirements."
"Truly, we do want practical guys, but ‘practical guys with a PhD’."
"I have a Ph.D. in Chaos Theory - not much direct use in industry - but it shows dedication."

R. Analyst & CEO, IT security company, “Information Security Research & Analysis"
"Actually, our ‘own’ security isn’t very pragmatic because it is too complex & scale, but we assume we are a bigger target and take extra steps."

R. CEO, IT security company, “For a more secure society”
'I use a WM6 phone to read my mail. That F*!#* thing has no option to disable things for better security.'
'We only do regular internal audits, and the results have been providing quite a lot of work already. So I will leave it as is.'

C. (social-engineer.org)
"Thank you for those tips. I just moved server.... So it was some stuff i overlooked"
"We went through and removed some mods added some other sec, hopefully ll good"
You are very concerned with our security, and have internal departments handling all aspects.

"Thank you for accepting our conference call invitation. I'm sorry, but we did not look into the details of the security breach reported to us a few days ago.

"Our software is very well tested, it is not possible to gain access to our secure certificate back-end database. So we are not interested in any alleged specific details about a faulty gateway for the ARM corporation. Thank you for your time, goodbye."

ARM Corporation:
"Thank you for taking time to use ARM's online contact form. Your request has been sent to the relevant representative within ARM and has been assigned reference number 10321"

"Produced By Microsoft Exchange V6.5: cam-exch2.emea.arm.com [10.1.255.58]; Your message was deleted without being read on Monday, February 10, 10:11:01 AM (GMT)"

E. Hired security officer at power company (which has one Nuclear power plant)
"I am CISA / CISSP, with 30 years of security experience, university lecturer. According to others an authority in the field."

"For customers we use all technical resources available to our profession, we have experienced security architects and we let our systems regularly be tested by the best ethical hackers there are in NL and abroad!"

"We are always looking for professionals who keep us on our toes, so surprise me with your knowledge and expertise!"

"You can’t see how we do our security just by looking at my website, which is of a much lower standard."

"Your bias I can not understand, nor why gcic.nl kicks against the profession."

Dr. W. CISSP LL.M, Head Info Sec. Strategies & Policies, Chair FI-ISAC
"We pass the intense official security audits, therefore we are proven to be secure!"

"We acknowledge that the reported structural flaws have been verified internally and our departments will handle it."

"We are perfectly capable of handling security matters internally, and do not require any input from outside, at this point in time."

B. (Verdasys) + D. (Verdasys) / Chief information security officer (In-Q-Tel)
"I am on the road but I did send this to IT with a note that we need to clean up any holes in our own infrastructure. I am most concerned about our own internal infrastructure that protects our software code and QA testing lab."

"I had a discussion with our IT folks and they have contacted a local company that the head of IT has worked with in the past. They were not surprised and were aware of many issues and had it on their agenda. They are going to start reporting it at our executive staff meetings on Monday to show progress so I can follow along. I thank you for the alert so I could move it up the priority chain of items they were working on."

Drs. M. CISA CISSP, Chief Architect Risk & Security, Author & Lecturer, Jericho Forum advocate.
"The Advanced Self Correcting Structure document does have a general appeal. As a member of the upper management, I would be inclined to invite the author to share a little-bit more about that adaptive security solution."

"Most organizations know, or at least have a gut feeling that their security does not provide 100 percent protection again unlawful access. One of the biggest design flaws is the simple fact that most organizations have no idea what the value of their information is. Next to that, most security technology was designed for a specific context. That doesn't mean that these solutions will work well in every context, nor where the products designed to interact with products from other vendors. Most organizations have a multitude of point-solutions. Not the good makings of a protective shield (which was in most cases our design idea)."

"Send from my iPhone^ via mail^ with iPhone Mail (7E18)"

A. Head of Network Security Section (Secret Service, National Security Authority)
"First - thank you for the info you provided. We verified the info and did some further investigations, and then brought it to our IT dept.

As far as I know, corrective measures has been made to most of the issues."

"But as I said to you - this is outside the scope of my responsibilities, so my knowledge in this matter is somewhat limited."

Anyway - your input has set some much needed focus on the importance of improving information/IT security procedures.

I'd like to thank you for handling this in a professional manner."
"Never mistake knowledge for wisdom.
One helps you make a living; the other helps you make a life."