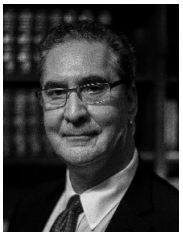
Why do cyber security programmes fail?

Received (in revised form): 8th January, 2019



Chris Moschovitis

was born and raised in Athens, Greece, and moved to the US in 1979. Here, he studied physics, computer science and mathematics, receiving his Bachelor of Science degree from The College at Brockport in 1983. Following his move to New York City in 1985, Chris was appointed director of academic computing at Pratt Institute, and in 1987 he was recruited by the O'Connor Group for the position of vice president of information technology. In 1989 Chris started his own company — The Technology Management Group — focused on providing independent technology and cyber security managed services. The company further expanded its services in 2004 by investing in emedia — a prominent, award-winning, internationally acclaimed interactive software development company — forming tmg-emedia. Today, tmg-emedia is one of the premier independent consulting companies in the USA. Chris is both cyber security (CSX, CISM) and enterprise IT governance (CGEIT) certified. He is a member of several organisations including ISACA, ISSA and the American Management Association. Chris is the co-author of the critically acclaimed *History of the Internet: 1843 to the Present*, as well as a contributor to the *Encyclopedia of Computers and Computer History* and the *Encyclopedia of New Media*. Chris' latest book *Cybersecurity Program Development for Business: The Essential Planning Guide* was published to critical acclaim by Wiley in 2018. He is an active speaker and writer, and delivers workshops on a variety of topics, including cyber security, information technology strategy, governance and execution, and digital and business transformation.

tmg-emedia, Inc., 274 Madison Avenue, Suite 1202, New York, NY 10016, USA
Tel: +1 212-381-4911; E-mail: Chris.Moschovitis@tmg-emedia.com

Abstract Despite the torrent of news about hacks, despite the clearly elevated awareness, despite the increasingly sophisticated tools and services, despite regulatory requirements, cyber security programmes are not always successful. Why do they fail? Where do they fall short? These should be key questions for everyone in business, government, technology and cyber security. If we know the problem with cyber security, and have ways of addressing the problem, why are we still failing? Without answers to these questions, all our work in cyber security amounts to building sandcastles.

KEYWORDS: cyber security management, cyber security failures, mistakes in cyber security, cyber security programme management

GETTING TO AN ANSWER: DOING THE MATHS

First, let us do the maths. In ISACA's 'State of Cybersecurity 2018' we read:

- 50 per cent of organisations surveyed believe that there will be an increase in cyberattacks;
- 80 per cent of those surveyed believe that an attack is likely or very likely.

The data points in a positive direction. Organisations are aware that the threat is real and imminent. It is the next piece of data that is so troubling:

- 31 per cent of those surveyed do not believe that their boards have adequately prioritised cyber security. That is, thankfully, down from 33 per cent the year before.

The respondents to this survey are ISACA members worldwide, across industries, with 67 per cent employed in an enterprise with

at least 1,500 employees. Traditionally we view enterprises with over 1,500 employees and with a board of directors as 'top tier' in terms of sophistication, governance and resources. When one-third of such organisations report their boards are not taking cyber security seriously, then everyone downstream should be running for the hills.

This is not the first time that alarms have been raised about cyber security programmes. To be sure, there are several excellent articles addressing a multitude of technical failures, as well as issues with cyber security awareness, cyber security management and implementation of cyber security controls. A small sampling includes:

- In their 2018 White Paper '2018 State of Security Operations', Micro Focus Cybersecurity Services reported: 'Historically organizations have struggled with satisfying the objectives of their cyber defence investments. Most security operations centres continue to be over-invested in technologies, often failing to take full advantage of each tool's capabilities. In spite of heavy technology investment, many struggle to prevent, detect, respond, and recover from cyber security attacks' and 'only 5% of assessed organizations are operating at recommended target levels of capability and maturity';[1]
- Varonis, in their '60 Must-Know Cybersecurity Statistics for 2018' reported '70% of companies have over 1,000 stale sensitive files', '21% of all files are not protected in any way' and '65% of companies have over 500 users who are never prompted to change their passwords';[2]
- Verizon, in their 2017 'Data Breach Report' wrote: '61% of breach victims of 2017 were businesses with under 1,000 employees'.[3]

Still, such problems remain, even as cyber security executive awareness inches closer and closer to maturity. Why? Where are the breakpoints?

To answer this question, we need to look at each major phase of cyber security programme development, understand the pitfalls, and recommend remediation steps on a phase-by-phase basis.

PHASE I. ASSET CLASSIFICATION AND ASSET VALUATION

When we start any cyber security programme, our first step is to get a thorough understanding of what are the assets that we will be protecting. Typically, they fall into one of the following classes: *data*, *hardware*, *software*, *systems*, *processes* and *workflows.* For each one of these assets, we must collect a set of asset metadata that should include (at a minimum) the asset owner, the asset custodian, its location, its confidentiality classification, its impact classification, the maximum tolerable downtime, its recovery point and time objectives and a list of resources associated with this asset.

This is a lot of work. A lot of hard, tedious work. Nevertheless, it is essential work.

Who is responsible to perform all this work? Two people: the asset owner and the person responsible for developing the cyber security programme — ideally the Chief Information Security Officer (CISO) or one of the senior cyber security analysts.

This is where the first serious gap appears.

Frequently, the asset owner, aka the 'business unit owner', is misidentified. For example, a typical mistake is to assume that the company's highly competent financial EVP is the 'owner' of the finance department. Not always the case. Frequently, the 'real' owner may be the controller along with other leads within finance (eg treasurer, AP/AR director, etc.) An honest mistake with catastrophic consequences.

Why? Because the VP of finance, as highly competent as they may be, may not be sufficiently 'in the weeds' to give you a

realistic impact classification, or an actionable maximum tolerable downtime, or a realistic recovery point objective.

There are other errors that can be introduced during this process: omissions, misclassifications, misattributions. For example, finance departments are notoriously ill-equipped in handling and valuing digital assets. Or, for another example, they may not even consider a certificate an asset. All these errors can be avoided, or at least minimised, when you are partnering with the right asset/business owner and you marry their expertise to yours.

How do we get asset classification and valuation right?

For one: Dig past the title. Ask to speak with the people who are directly responsible for business-critical functions, not their manager.

Then: Read the culture. Ask around who is the 'go-to' person when you have a critical issue within each business unit. Do not just go by the organisational chart, do some detective work. Of course, you will review the work with the EVP. Of course, you must secure their blessing. But, make sure you have analysed the full and detailed picture, not a picture from the 50,000-foot view.

Finally, be thorough. Turn over every rock. The certificate example is a good one. Do you know how many certificates are around? When do they renew? Who is managing them? Who is their 'owner'? Yet, a compromised certificate will be all that is needed to gain the trust of a server.

PHASE II. THREATS AND VULNERABILITIES

The next phase in developing a cyber security programme is taking a close look at threats and vulnerabilities. In the interest of oversimplification, when we are asking the questions 'Who's out to get me?' and 'How likely is it?' we are essentially performing threat analysis. When we are asking the questions 'How easy is it to get me?' and 'How can they get to me?' we are exploring our vulnerabilities.

The core output of this work forms a specific risk analysis, generates a risk register and specific risk assessments.

Once again, this endeavour requires the partnership between business stakeholders and cyber security professionals. And, as with the previous phase, the work is frequently tedious and exhausting, and also absolutely critical to a cyber security programme's success.

It is at this stage that multiple errors can be introduced.

First, business people can, and frequently do, underestimate the threats. Most common? 'No one is out to get me! Our business is too small!' or, 'There is no threat — no one has attacked us yet, so …'

Another example is ignoring a vulnerability because of some 'legitimate' reason. Here is one that may sound familiar: 'Oh, that system was an experiment, and it is no longer in production. We have no need to patch it.'

Remember: If it is connected to your network, it is a vulnerability.

Another common excuse? 'We cannot patch that server because our "old database" system will not work.' Perhaps so, but have you implemented any controls to work around this vulnerability? What are they?

How do we get vulnerability assessment right?

The truth of the matter is that you can do a lot more about the second and third examples, the 'non-production' system and the old database, than you can about business owners proclaiming immunity and sticking their heads in the sand.

For examples one and two, the key is to get it all down on paper. Be thorough. Leave no stone unturned. Audit as you go and uncover and document all the vulnerabilities. Engage with the business stakeholders and your technology partners, and do not rest

until you feel you have been exhaustive in your vulnerability cataloguing. Then, engage a third party vendor and have them perform vulnerability tests.

Work within that reality and it will serve you very well. It takes time and data to convince people to act. The first step is to have the data. Then work with people over time to shift attitudes around what can and cannot be done.

In the case where you have business owners that are in denial, your task becomes exponentially more difficult. Frequently, CISOs perform a well-rehearsed and documented 'fact attack'. Unfortunately, this is not an exercise of 'let me drown you in facts and figures'. Remember the adage: 'A man convinced against his will is of the same opinion still.'

With the head-in-the-sand crowd, your best — if not your only — chance is to attempt to engage on a personal level first. Establish trust, demonstrate that you have their interests first and foremost. This is not about rolling out some fancy cyber tech speak. This is about talking person-to-person about risk and risk management.

This requires trust, empathy and engagement. Not always the strongest suit of technologists, but always the most useful.

PHASE III. CONTROLS AND INCIDENT RESPONSE

After all the work and knowledge gained in the previous phases, the business is ready to crystallise a defence-in-depth strategy by implementing layers of *preventative*, *detective*, *corrective* and *compensatory* controls. Keep in mind that rolling out an active defence (the creation of honeypots and hacker traps that waste an attacker's time and can help with detection and identification) is an important consideration here, depending on resources and scope and in perfect alignment with a defence-in-depth strategy. Be very careful, though, since these types of active defence measures are encumbered by legal and regulatory constraints. Best advice is to always check with your legal counsel first, prior to deploying anything that may be considered suspect.

At the same time, and part-and-parcel with our business continuity and disaster recovery plans, is the incident response (IR) plan. The IR plan will address identifying incidents, containing them, treating them and recovering from them.

The possible errors in this stage are many and mostly come in governance, resources and skill level.

Let us start with the most obvious error: having IT pick and implement controls.

Many business owners can be blind to the inherent conflict of interest in such a set-up: cyber security is about risk management; IT is about value creation.

Next up: picking the wrong controls, or — worse yet — picking too many controls. Frequently, both CISOs and CIOs do not talk enough between them, and as a result you can find an enterprise that has layers of duplicate controls from different vendors, potentially with conflicting configurations. Which brings us to the next possible error.

Configuring the right controls, the wrong way. A typical excuse for this is budgets. We had the budget for the fancy IPS/IDS/SIEM toaster-microwave-oven (*capital expense* [CapEx]), but we could not get approval for professional services to instal and configure it (*operational expense* [OpEx]).

Finally, the truly horrid: no incident response plan, or a poorly designed incident response plan (aka checklist approach), or an incident response plan that is 'on paper' only, with no training, no validation, no testing or regular revisions.

How do we get controls and incident response right?

The first thing to understand and to communicate to the business is proper governance: what are the different roles and who wears which hat. The business needs

to understand the fundamental duality of IT versus cyber security:

- IT creates value;
- Cyber security protects value.

IT professionals are the custodians of value generation: information technologies.

Cyber security professionals protect that value.

The examples that you can use in explaining this are endless. Pick the one that works best for your business culture. I developed the 'team coach versus team doctor' analogy. The team coach always wants the best player on the field, frequently willing to dismiss an injury as 'trivial'. The team doctor is always interested in the health and wellbeing of the athletes and will therefore be much more reluctant to approve a player's entry back in the game following an injury. I find that most people understand this simple analogy in terms of value creation versus value protection. There are, of course, many others. I urge you to use the one that best reflects your company's culture. Pick the one that works for you, and then discuss with your stakeholders why the team doctor cannot possibly be reporting to the coach. Instead, both need to be reporting to the only entity that can accept risk: the team owner. Notice the use of 'discuss' as opposed to 'explain'. This is an important distinction, and something that you should be very sensitive about. No C-level executive wants to be 'explained at'. Most, though, would welcome an enlightening and informative discussion.

Once you have the proper governance in place, you can focus on the more technical domains of control strategy, deployment, optimisation and the creation of a living incident response plan.

Do not attempt to do this in isolation. To get controls and incident response right, you will need skilled, experienced cyber security professionals, working in partnership with their IT counterparts. Cyber security and IT are two parallel tracks that your business is riding on. One simple misalignment here and this train will derail.

This part of a cyber security programme is technically complex. There is the obvious need to make sure that control selection is appropriate and business-pragmatic and that control configuration is done right. You and your team will need all the help they can get. There is no room for 'tech ego' in this exercise.

Make sure that you involve expertise from vendors, partners and colleagues throughout this process. It is the cyber security professional's responsibility to be up-to-the-minute informed, inclusive and solicitous of expert advice. Isolating yourself and 'going at it alone' is a recipe for disaster, and a callous disregard of best practices and common sense. Remember, this need not be costly. There are many forums and resources available to you for free. Use them.

Finally, you need to focus on any CISO's magnum opus: the incident response plan. Obviously, no two plans are alike, since they reflect the specifics of each company, but they do share common sections, just like any good disaster recovery and business continuity plan does.

The problems with incident response plans can be many: hastily made, incomplete and worse of all, untested. Everything rides on the incident response plan. It does not matter how much work, cooperation, or good intentions have gone to the cyber security programme thus far. What matters is that a solid, tested and 'living' cyber security incident response plan is in place.

Why? Because the truth of the matter is that no matter what, no matter who and no matter how, if you are the target of an advanced persistent threat (APT) you will be breached. Therefore, the only thing that matters is how prepared you are to respond to such an incident. How fast can you detect a breach? How fast can you recover? How well can you meet your recovery time objective (RTO) without blowing the maximum tolerable downtime (MTD)

and how completely you can get to your recovery point objective (RPO)?

Again, to maximise the chance of success you need to be as inclusive as possible. Your team must ensure not only that the correct technical skills and components are in place, that vendors and their SLAs can be met every single time, but also that the business is fully on board, trained and in sync with the plan. Also, it is important to test the plan as exhaustively as possible, process-by-process, workflow-by-workflow, system-by-system, and ideally invite an independent third party to review the plan for you. A third party, outside of your reference frame, can provide invaluable guidance in making your plan as robust as can be.

When an incident happens, everyone needs to be singing from the same song sheet: communications needs to be aligned with legal, which needs to be aligned with cyber, which needs to be aligned with the business and the executive chain.

Panic has no place in incident response, and the only way to remove panic is to train for it — again, and again, and again.

PHASE IV. LIVING CYBER SECURE

It would be naïve for anyone to assume that if we avoided all the errors during programme development, we would instantly achieve cyber security nirvana. The programme, no matter how well conceived and executed, still has a huge vulnerability.

What is this single, persistent point of failure? People.

I would argue that even if a technological cyber security nirvana is achieved through the use of artificial intelligence, machine learning, quantum computers and any other yet-to-be-imagined technological miracles, even then we would still have the one, persistent, single point of failure. People.

The persistent people problem takes many forms: from the boards that ignore cyber security, to the executives that pay it lip service. From the managers who ignore cyber security requests, to the employees that violate policies. From the 'I know best' ego-driven cyber security professionals, to 'IT knows better' techs.

People have been, are and will be cyber security's biggest asset and worst nightmare. Depending on how you approach, disseminate, communicate and manage your programme, you may be able to influence which side 'your' people end up.

How do we get living cyber secure right?

The problem does seem overwhelming. How do you solve the 'people' singularity?

Some suggest keeping your head down and doing your work and accepting 'what will be, will be'. Others argue that education is the answer. Others want more intensive training, awareness and tying compensation to cyber compliance. Some blame greed and single-minded fiscal-performance focus. Others curse at the speed of technological change that is leaving people in the dust.

There are still others, much more studied in the understanding of human behaviour and thinking, who suggest methods for convincing people of a position (eg the legendary Dr William McGuire's 'inoculation theory'). In this way of thinking, we need to create the necessary space and climate for discourse and understanding.

It is too bad that neither ISO nor NIST have a 'trust framework' yet. But other disciplines do. Psychologists (organisational and clinical), anthropologists and sociologists have written volumes on the subject. Perhaps spending some time understanding humans as much as we understand computers may yield better results all round? Traglia and Delia seemed to think so when they presented 'Cybersecurity Inoculation' at the New York State Cybersecurity Conference and Symposium on Information Assurance in 2017. Their work is an excellent example and should be required reading for all CISOs.

In my experience, I have found one thing that works almost all the time: strong

engagement. With engagement you build trust, establish communication channels, and develop durable bonds of respect with the person across the table from you. Even though he or she does not 'speak' the same cyber language, may not understand the technical nuances, has no time to deal with yet one more thing and may be afraid to look ignorant or needy — with the right trust framework in place, you can talk to each other.

This approach works and has had an incredible side effect: it teaches us more about how to be effective in delivering businesses the right solution over all the skills, training and experience combined.

And, in my experience, it has kept many a cyber security programme alive and well.

IN SUMMARY

A quick way to refer to all this is by following Table 1.

References

1. Micro Focus (August 2018), 'State of Security Operations 2018 Report', available at https://www.microfocus.com/en-us/assets/security/state-of-security-operations-2018-report (accessed 27th February, 2019.
2. Sobers, R. (January 2019), '60 Must-Know Cybersecurity Statistics for 2019', Varonis, available at https://www.varonis.com/blog/cybersecurity-statistics/ (accessed 27th February, 2019.
3. Verizon Digital Media Services (March 2018), '2017 Verizon Data Breach Investigations Report', available at https://enterprise.verizon.com/resources/?page=1/ (accessed 27th February, 2019).

Table 1: Why do cyber security programmes fail — quick reference

Cyber security programme phase	What can go wrong?	Getting it right
Asset classification and asset valuation	• Misidentified business unit owner. • Asset missions, misclassifications or misattributions.	• Dig past the title. • Read the culture. • Be thorough. Turn over every rock.
Threats and vulnerabilities	• Underestimated threats by the business. • Unpatched 'obsolete' systems. • Insecure legacy systems still in production.	• Engage on a personal level. Develop trust and empathy with the business leaders. Explain from their side. • Audit as you go. • Again: be thorough. Turn over every rock. Insist on comprehensive systems vulnerability assessments.
Controls and incident response	• Governance, resources and skill level errors. • Picking the wrong controls or — worse yet — picking too many controls. • Configuring the right controls, the wrong way. • No incident response plan or a poorly designed incident response plan.	• Establish proper governance: separate value creation from value protection. • Break from isolation. Insist on skilled, experienced cyber security professionals. • Eliminate 'tech ego'. • Be inclusive: make sure that you involve expertise from vendors, partners and colleagues throughout this process. • Ensure a solid, tested, trained, verified and 'living' cyber security incident response plan is in place.
Living cyber secure	• Remember 'the' single, persistent, point of failure? People. • Boards ignoring cyber security. • Executives paying it lip service. • Managers who ignore cyber security requests. • Employees who violate policies. • Ego-driven cyber or IT staff.	• Engagement. • Use a multidisciplinary approach (psychology, sociology, anthropology). • Understand cultural dynamics. • Build trust. • Establish communication channels, both formal and informal.

Keep this table as a reference. If you stay committed, execute thoroughly, are decisive, engaging and inclusive, the odds that your cyber security programme will succeed rise exponentially.