IGF Best Practices Forum on "Establishing and Supporting CERTS for Internet security

Report 2. CERT costs

Note. This report joins the comments on the online forum. As there were distinctive topics that were discussed, they are presented separately. Entries are presented in the order of arrival. First the contributor is mentioned and where appropriate within brackets the person responding to is mentioned, e.g. (Wout). The affiliation of a respondent is not mentioned, as he/she may be giving a personal point of view or not. As consultant to the group this is impossible and not necessary to ascertain.

Adli Wahid

Thanks for all of the interesting discussion and feedback on various topics so far. Another subject that I'd like to bring up is the cost aspect of running or operating a CERT/CSIRT.

Obviously we know this depends on a lot of factors or activities of the CERT/CSIRTs. However I think it would be useful to give some general ideas to the other stakeholders for instance:

a) What are the cost-components for running a cert/csirt
b) Priorities - What you must invest on, what sort of things are optional, what are the freebies etc
c) Strategies for getting funds or securing resources
d) Etc - Perhaps those with non-cert/csirt background and ask more questions related to cost here as well)

In the past, I always get the question on the cost of setting up for a 'monitoring centre' (with big flashy screens and blinking world map :-) when in fact we know in reality this is not really for mandatory to have in order to do CSIRT work.

There was a time also when the CERT/CSIRT that I was part of spent a lot of money to subscribe to threat intelligence, not realising (after speaking to other CSIRTs) that some of these things are already available in the public domain or can be accessible once you develop trusted relationships with teams/groups.

If any of you can share your experience or observation on this please reply to this thread.

Tom Millar
In my limited experience, overhead (facilities costs) and salary/wages/benefits are the largest cost center of a CSIRT. Technology expenditures (pipe, iron, or paper) are not as big of a deal, especially if you do not initially invest in a liquid-cooled malware lab or the star trek watch center as Adli describes. Also, tech prices go in the opposite direction of labor rates and leases over time. When you go to buy the same thing five years later, the tech and bandwidth is cheaper, the labor is usually more expensive, and the office space and furniture are almost always more expensive (all in real terms, not nominal currency values).

Two more important cost centers are travel and training. To be good and to retain the best people, you have to be able to send them to training events. This seems frequently underestimated by a lot of CSIRTs and SOC organizations. If you don't give your (already expensive) cybersecurity professionals the opportunities to train and develop, they will either stagnate in place or find other opportunities. The total cost of training and travel budget is a relative pittance compared to salary and benefits, but it tends to get a lot of scrutiny, in my experience.

Your legal and regulatory certification and accreditation environment can also drive significant costs. If you can only buy things that meet CC EAL4 or only procure services from companies that meet specific CMMI or ISO criteria, it can lead to quadruple+ costs for certain tools and labor.

Giant "I am just a guy, this is not the official position of DHS or the USA" disclaimer goes here.

Tom Millar

One other thing that surprised me this year in talking to some more "unusual suspects" from our critical infrastructure CSIRTs and the new ISAC partners standing up is that the salary norms for experienced cybersecurity professionals are quite hard to swallow in many sectors. In the US, we are talking about CSIRT jobs starting in the upper five figures. Many sectors find it very difficult to accommodate an "entry level" position in that range. So any initiative to improve CSIRT capability for infrastructure owners and operators may need to do one or both of:
1. Increasing the talent pool through secondary vocational and university education programs
2. Helping businesses develop (and live with) a specialized pay scale for their cybersecurity staff

Maarten van Horenbeeck (on Tom Millar)

Great point, Tom. I agree that personnel cost is usually the most significant expenditure of a CSIRT.

One other thing I'd raise is that cost is also directly related to the type of services a CSIRT offers. RFC 2350 lists out a number of services that a team may offer to its constituency:

https://www.ietf.org/rfc/rfc2350.txt

CERT/CC has a much more comprehensive list here:
http://www.cert.org/incident-management/services.cfm?

In this list, there are services which are simply much more expensive than others. These can be capital expenditure, such as expensive hardware when a CSIRT incorporates an intrusion detection service. On the other hand, cost can also be a more operational expense, when it is associated with the
depth of expertise in a service.

Getting one very skilled engineer in a more rare area of expertise, such as vulnerability analysis or reverse engineering, and growing their level of expertise can be more expensive than hiring several entry level analysts. Depending on the constituency, this type of service may be more, or less important.

Sometimes there are opportunities there for CSIRT teams to share capability. One CSIRT in a region or industry could specialize in one capability, agreeing with another CSIRT that it will specialize in another area. This makes that the regional community benefits from several areas of expertise, while the investment does not need to be duplicated across each CSIRT.

This type of load sharing becomes more difficult when it pertains to matters of great confidentiality, but in most CSIRT I’d argue that this is actually the exception, not the rule.

Sharing of capabilities can be a manual effort (calling in help from another team to investigate a complicated case) or something automated- the Malware Information Sharing Platform (MISP) and FISHA/NISHA are good examples of projects that enable this. If you have any type of shared repository, where participants can receive, and either contribute or re-share information adding additional context, you can achieve this goal.

Andrew Cormack (on above)

I’m no longer involved in CERT spending, though my experience from a decade ago was definitely that staff and travel (aka trust building) costs were the big budget costs.

However I get the impression that one area where Moore’s law doesn’t mean equipment price inevitably drops if you just wait is if you’re buying kit to monitor national-scale networks. Janet is currently running at 100Gbps all around the UK and boxes that can make sense of that firehose make even Tom’s analyst costs (don’t show those to my colleagues, please!) look cheap. Though, as we’ve already mentioned, not many *national* CERTs have that problem as they generally don’t run the extreme speed networks anyway.

Andrew Cormack (on above)

Just in case others don’t know the resource that can save you lots of money on information sources: see


Apologies to Adli that we clearly didn’t point this out to him when he needed it :(

Patrick Green
Here is my $2_local_currency...

As other people have mentioned, the main cost factor will be human resources. However, there are a number of things to think about.

Will the team be operational or advisory (this leads into the whole National CERT discussion)?

What services will they be running for the community (as mentioned, they can announce this in their RFC2350 profile).

What is the size of the constituency? I’ll delve more deeply into operational teams from now on, I work on a guidance figure of about 1 CERT person, per 10,000 machines - assuming business hours coverage. In an ideal world...

What are the hours the CERT need to be responsive? Can you build a follow the sun model, or do they have to be local?

In terms of priorities for hardware for operational teams;

How many choke points are there on the network - how many places do you want to monitor? This starts to affect the hardware costs.

What is the strategy for monitoring them (given the speed)? FOSS or Bought-in systems?

What support systems can you take from the overall environment (ticketing systems etc) and how many need to be run by the team?

What does each service the CERT will provide need (malware lab? Threat feeds?)

Jean Robert Hountomey

Also - conference budgets. I think this has been mentioned - don’t underestimate the requirement for people to go to conferences, this is the main way that trust relationships are built, and are priceless in terms of making the CERT more effective.

As for funding strategies - metrics - show the number of problems that are out there, externally if you don’t have any internal numbers (who does the business measure itself against) and start building the slide decks and presenting the results :-)

More questions than answers, but I hope it adds some value to the discussion!

olivierkouami
+1 to Jean Robert

Jean Robert Hountomay

I would like to add another cost I like to call "Soft Skills" (can be under training) where I put items like : Communication, Customer management,
Stress handling and even Language...
(Asking for example a non English speaking team member to take English reading, writing and speaking classes is an important budget line that was not obvious until we faced it).

JACQUES TANOH BEUGRE

I would like to stress the need of training funding in the budget; training the team not only on response and analysis but also on being good with the tools and learning new tools. We faced an interesting issue a few months ago where we moved from responding and assisting with few incidents a month to daily analysis while the team was not prepared and trained to deal with that amount of data. We had to learn additional tools, scripting and programming and take few trainings.

Also budgeting the cost of employee retention is important. Another one is the cost associated with having a process to get new staff up to speed and ready.

In addition, lessons learned from a tight budget with approval seeking for everything teach us to make provision to cover few unforeseen strategic issues.

I wonder how other teams deal with responding to strategic issues that were not budgeted.