Forensics Team Staffing Considerations

Table of Contents

Staffing ............................................................................................................................................ 2
Staffing Categories .......................................................................................................................... 3
Staffing Considerations – Cost ........................................................................................................ 5
Staffing Considerations – Sensitive Data ........................................................................................ 7
Staffing Considerations – Logistics ............................................................................................... 11
Notices .......................................................................................................................................... 12
So here's some considerations for staffing. If you're thinking about setting up a team and you're looking to hire some people or whether or not to hire people is what you're looking at.
**Staffing Categories**

**Position** | **Staffing** | **Handling**
---|---|---
Incident Handlers | includes computer security incident responders | use a wide variety of forensics tools
IT Professionals | support staff and system administrators | use a small number of routine tools (log monitoring, network troubleshooting, etc.)
Investigators | may include legal advisors and human resource employees | typically deal with allegations of misconduct and/or criminal activity

**014 So generally speaking, we've broken this down into three categories. We had the incident handlers, right. These are the folks who actually get the hands on the tools. You know, the computer security incident responders, those type of folks, is what you're looking for. That is a specific skillset. Generally people with an IT background don't necessarily have these skills.

IT professionals. That's kind of really broad, actually, but we're talking about the support staff, the system admins, the network admins. Those are the folks that we're looking at
there. And...right. Some of the tools that they use. They also monitor logs, perhaps for different reasons, right. And they do network troubleshooting, et cetera. And then you have your investigators. And usually these folks are either in the legal area or even human resources, if you’re talking about insider threat. Those folks will be a part of the investigative team. And they typically deal with the actual allegations of either misconduct or some sort of criminal activity.

So for the team itself, you’re actually looking at mostly the incident handlers for a particular team.
Staffing Considerations – Cost

A forensic specialist can be an expensive investment.
  • Average salary for Digital Forensic Examiner: $92k

Determine if in-house forensics is more cost-efficient than third-party forensics.
  • Based on frequency and type of services

Training is a key cost when building a digital forensics capability.
  • Just as rapidly as technology advances, so does the need for training on new tools and methods.

**015 Okay. So staffing considerations due to cost. As you could see there, the big number, $92,000, that's on average. Got that number from indeed.com. And that is an average, right, for a forensic specialist. You've seen the Engineer 1, Engineer 2, Engineer 3, Engineer 4. So that might be a digital forensic examiner, two and a half-ish, might be where that is. So if you get somebody brand-new that has some of the education and some training, maybe even a certification, you're looking at the lower end of the scale. And, of course, you have people that do the data carving and they actually go in and pull up, you know, break apart
platters of hard drives. Those folks are going to be a little bit more than that.

So here's the other piece of staffing or deciding to whether or not to have your team is...Would an in-house forensics team be more cost-effective than a third-party forensics team? And this is all based on the frequency and the actual type of services that you'll be needing, right?

So if you have an incident quite often, and you have to send many of your regular, if you will, IT folks off to try to investigate these things, maybe it would be cost-effective to have your own in-house team developed. And also if you're talking about possibly chasing down information of checking a browser history or a proxy history versus actually breaking down platters of a hard drive or going after things that have been semi-erased, that's also an area where you might want to consider that, is, you know, might be better to have the in-house forensics team. Then you can have more skillsets built for this particular thing.

So going along with the equipment and the software that you'll have, the training will be a pretty big key as well, because not only do you have to train them up at the very beginning, but there's always the cost of recurring training, right? Because there's always going to be updates, there's always going to be new things that are going to be coming down the pipe.
So these are all cost ideas to consider if you're going to be looking at developing an in-house team, or in general, a forensics capability within your own organization, and ideas to think about if you're thinking whether or not you just want to work with a phone number or do you want to have maybe one or two people versus a full-fledged team?

**Staffing Considerations – Sensitive Data**

Certain industries may have certain regulations and/or policies that require specific sensitive data handling.

- Health-care – HIPAA
- Finance – PCI DSS, Securities & exchange commission
- Government – Classified Information, FISMA PII

Even if regulations do not mandate staffing, an organization may have intellectual property that would be best handled internally.

Internal incidents may require a third-party to reduce conflict of interest with regard to the investigation.

**016 Okay. Another consideration for staffing is sensitive data. So certain industries have regulations or requirements that require you to take care of certain data a certain way.**
Right. The healthcare industry has the Health Insurance Portability and...

Student: Accountability.

Instructor: Accountability Act.
Thank you. Had to remember the other A there. So HIPAA information is very, very sensitive. And I used to be HIPAA certified. And if there's an incident with HIPAA information, we're talking tens of thousands of dollars to hundreds of thousands of dollars, based on however many incidents that you have. And it could be each patient's information, could be the tens of thousands of dollars apiece. So we're talking very, very important and obviously a very high risk level, right, if your organization deals with HIPAA data.

So in this case, maybe you want an in-house, because you want people who take care of it all the time. You don't want some third-party person showing up that really doesn't know HIPAA and, "Yeah, I just got HIPAA certified yesterday," right. You don't want that kind of a team that shows up and maybe make the situation worse. So you want to pay attention to those things. If you're heard of PCI DSS, right, that's the payment card industry. It's credit card information, Data Security Standard. And then, of course, there's the Securities and Exchange Commission. You don't want your company's information of possibly merger and acquisition to leak out. So if you have any issues with a possible investigation, you may want in-house
personnel to take care of this, because they'll be aware of the situation and they're already there.

And for the government, there's classified information, of course. You obviously don't want the secret and the top secret stuff to get out. You've got to make sure your folks, you might want to make sure, that the folks internally are the folks. Although there are quite a few obviously contractors that deal with confidential and classified information. So there's some. I would think there would be more people that are accustomed to dealing with classified information than there are possibly the other two.

And the FISMA, Federal information Security Management Act, put some strict guidelines on the PII I mentioned earlier, personally identifiable information. This is the information that maps to you as a person, right? Your phone number, your address and such. Anything that especially a governmental organization maintains on you, they have strict regulations on how long they can keep it if you no longer work there. Where they have to store it and the security requirements for that.

So even if the regulations don't necessarily mandate it, when a organization may have intellectual property, right, and they also may have their process that they have. And their corporate knowledge in general, how their processes work.
That’s very important to a lot of companies. So again, you may be looking at keeping that in-house, because you expose any of the intellectual property information to outsiders, it could be a risk for somebody to take that information and share that with somebody else, to their benefit. Right.

And then on the other side of that coin is that if you have an internal incident, right, possible insider threat, you may want a third-party organization to come in, because you don’t know how far it goes and how wide it goes. You may want people who are objective to the whole situation and they can do the investigation and the forensics piece without worrying about does somebody know somebody else, is somebody a friend of somebody else, and you’re not sure if the actual investigation is going to be done in an objective manner. So that’s the other side of that is that you may want to have a third-party come in that doesn’t know anybody at the company.
**017 Okay. And then there are the logistics of having a team either on site or remote. Right. On-site forensics team may not be cost effective. If you have 20 global offices, how many local teams can you have? Can you afford to have that many digital forensics folks? Probably not the case. So you may be looking at teams in regional area, so they can reach out to specific areas and get there relatively quick.

The off-site forensic teams may not give you the response times you need. Depending on the type of company you are. If you’re a bank. If you’re dealing with stocks. And
certain other industries. Maybe you need a response time that’s just that much faster and you’re just going to have to spend the money to have the teams on the site, on-site. So something to consider on that as well.

Notices

© 2016 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government’s rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark owned by Carnegie Mellon University.