

فهرست عناوین

20	1. امنیت فن آوری
20	1.1. خلاصه فصل
20	1.2. مقدمه
21	1.3. معرفی موسسه پونمن
21	1.3.1. هزینه‌های ناشی از سرقت اطلاعات
22	1.3.2. توزیع هزینه‌های تخلقات رایانه‌ای بر اساس اندازه سازمان
22	1.3.3. تحلیل‌های هزینه بر اساس تعداد پست سازمانی
23	1.3.4. متوسط زمان بازیابی سرویس‌ها
24	1.4. مفاهیم پایه
24	1.4.1. ریسک
25	1.4.2. سرمایه‌ها
26	1.4.3. تهدیدها
26	1.4.4. آسیب‌پذیری‌ها
27	1.4.4.1. انواع آسیب‌پذیری
27	1.4.4.2. اهمیت آسیب‌پذیری‌ها
29	1.4.4.3. علت آسیب‌پذیری‌ها
29	1.4.4.4. منابع نا امنی یا آسیب‌پذیری‌ها
30	1.4.5. رابطه بین تهدیدها، کاستی‌ها و ریسک
30	1.5. الزامات اساسی چارچوب مدیریت ریسک نرم افزار
31	1.5.1. درک حوزه تجارت و کسب و کار
32	1.5.2. تشخیص ریسک‌های تکنیکی و تجاری
33	1.5.3. تحلیل و اولویت‌بندی ریسک‌ها و تولید مجموعه‌های مرتب
33	1.5.4. تعریف استراتژی تسهیل ریسک
34	1.5.5. انجام فعالیت‌های تاییدی و بازیابی
34	1.6. متدهای ارزیابی ریسک
35	1.7. تشخیص ریسک
35	1.7.1. گام‌های تشخیص ریسک
36	1.7.2. برخی تکنیک تشخیص ریسک
37	1.8. تحلیل ریسک
37	1.8.1. اثرات تجارت و کسب و کار



37.....	1.8.1.1 مدل DREAD
38.....	1.8.2 احتمال
39.....	1.8.3 ارزشیابی ریسک
39.....	1.9 طبقه‌بندی و اولویت‌بندی
40.....	1.10 متریک‌های امنیتی
43.....	1.10.1 تهیه متریک‌هایی مناسب امنیت سیستم‌های کامپیوتری
45.....	1.10.2 چالش‌های پیش روی پیشرفت تهیه متریک‌های امنیت فناوری اطلاعات
46.....	1.11 برگشت سرمایه در امنیت فن آوری
46.....	1.11.1 برگشت سرمایه و تحلیل ریسک:
49.....	1.11.2 مدل‌های برگشت سرمایه
49.....	1.11.2.1 مدل PayBack
50.....	1.11.2.2 مدل NVP
51.....	1.12 نتیجه‌گیری
52.....	1.13 سئوالات آخر فصل
52.....	1.14 منابعی برای مطالعات بیشتر
54.....	2. استانداردهای امنیت فن آوری
54.....	2.1 خلاصه فصل
54.....	2.2 مقدمه
55.....	2.3 استاندارد چیست
56.....	2.4 روند تهیه استانداردهای جهانی
57.....	2.4.1 زیر گروه امنیت سازمان ITU
57.....	2.4.2 زیر کمیته تخصصی JTC
58.....	2.4.3 مروری بر چگونگی ساختار JTC
59.....	2.5 معرفی استانداردها
59.....	2.5.1 ISO/IEC 24765: 2010 لغت نامه مهندسی نرم افزار
59.....	2.5.2 ISO /IEC 2382-8 : 1998 لغت نامه امنیت فناوری اطلاعات
60.....	2.5.3 استانداردهای اولیه مدیریت امنیت
61.....	2.5.3.1 BS7799 اولین استاندارد مدیریت امنیت اطلاعات
63.....	2.5.3.2 استاندارد ISO/IEC 17799 موسسه بین‌المللی استاندارد
64.....	2.5.3.3 راهنمای فنی ISO/IEC TR13335
66.....	2.5.4 خانواده استانداردهای ISO/IEC 27000
66.....	2.5.4.1 ISO/IEC 27000

67	ISO/IEC 27001 2.5.4.2
70	ISO/IEC 27002 2.5.4.3
79	ISO/IEC 27003 2.5.4.4
80	ISO/IEC 27004 2.5.4.5
80	ISO/IEC 27005 2.5.4.6
83	ISO/IEC 15443 استاندارد 2.5.5
86	2.5.5.1 فرایند ارزیابی
89	2.5.5.3 مراحل ارزیابی
90	2.6 نتیجه گیری
90	2.7 سئوالات آخر فصل
91	2.8 منابعی برای مطالعات بیشتر
94	3. مهندسی امنیت
94	3.1 خلاصه فصل
94	3.2 مقدمه
97	3.3.1 دلایل نبود سیستم نظام یافته و زیر بنایی امنیت
97	3.4 امنیت اطلاعات چیست؟
98	3.4.1 امنیت در قبال ایمنی
98	3.4.2 برخی اهداف مهندسی امنیت
99	3.4.3 انواع سازمانهای مهندسی امنیت
100	3.5 ضمانت نرم افزار
100	3.5.1 تعریف ضمانت
101	3.5.1.1 سیستم نرم افزاری و خدمات
101	3.5.1.2 مبرا بودن از آسیب پذیری های داخلی و تصادفی
102	3.5.1.3 توانایی امنیتی مناسب برای مقابله با تهدیدهای محیطی
102	3.5.1.4 توان تحمل خرابی و بازیابی از خسارت
102	3.5.1.5 ایده ها و اهداف ضمانت نرم افزار
103	3.6 مهندسی امنیت
104	3.7 پیچیدگی تعاریف و لغات حوزه امنیت
105	3.7.1 سیستم
105	3.7.2 موضوع ، شخص ، مشارکت
106	3.7.3 اعتماد و قابلیت اعتماد
106	3.7.4 محرمانگی، حریم خصوصی و مخفی سازی و حفاظت از اطلاعات



107	3.7.5. صحت و درستی
107	3.7.6. وضوح
108	3.8. پروتکل
109	3.9. گذرواژه
110	3.9.1. انواع روشهای استقرار گذرواژه
110	3.9.2. کاربرد مسائل روانشناختی
111	3.10. مهندسی اجتماعی
112	3.11. کنترل دسترسی
113	3.11.1. کنترل دسترسی سیستم عامل
115	3.11.2. گروه یا وظیفه
115	3.11.3. لیست کنترل دسترسی
117	3.12. سیستمهای امنیت چند سطحی
120	3.12.1. نمونههای سیستمهای امنیت چند لایه
121	3.12.2. سیستمهای امنیت چند لایه آینده
122	3.12.3. مشکلات سیستمهای امنیت چند سطحی
122	3.12.4. قابلیت ترکیب
123	3.12.5. مشکل آبخاری
123	3.12.6. کانالهای مخفی
124	3.12.7. تهدیدات ناشی از ویروس
124	3.12.8. چند نمونه سازی
125	3.13. امنیت چند جانبه
127	3.14. درخت حملات
128	3.14.1. ملاحظات و ویژگیهای درخت حملات
130	3.15. نتیجه گیری
131	3.16. سئوالات آخر فصل
131	3.17. منابعی برای مطالعات بیشتر
134	4. مهندسی ارزیابی امنیت
134	4.1. خلاصه فصل
134	4.2. مقدمه
135	4.3. تعریف استاندارد ISO/IEC 15408
136	4.4. جایگاه CC
138	4.4.1. دیدگاه مشتریان در مورد CC

138.....	4.5 مستندات مهم
138.....	4.5.1 هدف مورد ارزیابی
139.....	4.5.2 الزامات امنیتی
140.....	4.5.3 ارتباط بین SFRها و اهداف امنیتی
140.....	4.5.4 الزامات ضمانت امنیت
141.....	4.5.5 هدف امنیتی
142.....	4.5.6 بسته‌ها
142.....	4.5.7 پروفایل محافظتی
142.....	4.5.7.1 نویسندگان پروفایل محافظتی
143.....	4.5.8 مستندات دیگر
143.....	4.5.8.1 تعریف مشکل امنیتی
143.....	4.5.8.2 خط مشی‌ها سازمانی امنیت و خط مشی‌های ابلاغی کشوری
144.....	4.6 مخاطبان استاندارد CC
144.....	4.7 ارزیابی در CC
145.....	4.7.1 انواع ارزیابی
146.....	4.8 تضمین ISO/IEC 15408
146.....	4.9 معرفی کلاسهای تضمین CC
146.....	4.9.1 کلاس APE
146.....	4.9.2 کلاس ASE
147.....	4.9.3 کلاس ADV
147.....	4.9.4 کلاس AGD
147.....	4.9.5 کلاس ALC
147.....	4.9.6 کلاس ATE
148.....	4.9.7 کلاس AVA
148.....	4.9.8 کلاس ACO
148.....	4.10 سطوح تضمین ارزیابی
148.....	4.10.1 سطح اول - آزمون کارکرد
149.....	4.10.2 سطح دوم - آزمون ساختاری
150.....	4.10.3 سطح سوم - بررسی و آزمون متدولوژیک
151.....	4.10.4 سطح چهارم - مرور، آزمون و طراحی به لحاظ متدولوژیک
151.....	4.10.5 سطح پنجم - طراحی و آزمون نیمه رسمی
152.....	4.10.6 سطح ششم - آزمون و طراحی تحقیق شده ی نیمه رسمی



153.....	4.10.7 سطح هفتم - آزمون و طراحی تحقیق شده ی رسمی.....
154.....	4.11 مهندسی ضمانت نرم افزار.....
154.....	4.11.1 اساسی ترین موضوعات در ضمانت نرم افزار.....
156.....	4.11.2 ارزیابی ضمانت.....
157.....	4.12 طراحی مدل های تجاری ارزیابی ضمانت نرم افزار.....
157.....	4.12.1 اهمیت و ضرورت طراحی مدل های ارزیابی تجاری به صرفه.....
158.....	4.12.2 طراحی مدلهای تجاری ارزیابی به صرفه.....
160.....	4.12.3 روند ساخت یک مدل ارزیابی تجاری امنیت.....
162.....	4.13 مرور مدلهای COST/BENEFIT.....
163.....	4.14 نتیجه گیری.....
164.....	4.15 سئوالات آخر فصل.....
164.....	4.16 منابعی برای مطالعات بیشتر.....
168.....	5. مولفه های عملکردی امنیت.....
168.....	5.1 خلاصه فصل.....
168.....	5.2 مقدمه.....
169.....	5.3 کلیات و ساختار بخش دوم استاندارد CC.....
172.....	5.4 کلاس ممیزی امنیت FAU.....
174.....	FAU_SAR.1، بازبینی ممیزی: قابلیت خواندن اطلاعات را از مستندات ممیزی ایجاد می نماید.....
175.....	5.5 کلاس ارتباطات : FC.....
176.....	5.6 کلاس پشتیبانی رمزنگاری : FCS.....
177.....	5.7 کلاس محافظت از داده های کاربری : FDP.....
185.....	5.8 کلاس تشخیص و احراز هویت : FIA.....
187.....	5.9 کلاس مدیریت امنیت : FMT.....
190.....	5.10 کلاس حریم خصوصی : FPR.....
192.....	5.11 کلاس محافظت از FPT : TSF.....
198.....	5.12 کلاس استفاده از منابع : FRU.....
199.....	5.13 کلاس دسترسی به TOE : FTA.....
201.....	5.14 کلاس کانال ها/ مسیر مطمئن : FTP.....
202.....	5.15 نتیجه گیری.....
202.....	5.16 سئوالات آخر فصل.....
203.....	5.17 منابعی برای مطالعات بیشتر.....

206	6. مولفه‌های تضمین امنیت
206	6.1. خلاصه فصل
206	6.2. مقدمه
207	6.3. کلیات
207	6.3.1. مولفه‌های تضمین امنیت
207	6.3.2. خانواده‌های تضمین
208	6.3.3. سطوح تضمین ارزیابی و ساختار آن
209	6.3.4. ساختار CAP
209	6.3.5. ارتباط بین تضمین‌ها و سطوح تضمین
210	6.4. کلاس‌های تضمین
210	6.4.1. کلاس ارزیابی هدف امنیتی : ASE
211	ادعاهای انتطابق ASE_CCL
212	تعریف مساله امنیت ASE_SPD
215	6.4.2. کلاس APE ارزیابی پروفایل محافظت
216	6.4.3. کلاس ADV توسعه
224	6.4.4. کلاس AGD اسناد راهنما
227	6.4.5. کلاس ALC پشتیبانی چرخه حیات
228	6.4.5.1. قابلیت‌های CM .ALC_CMC
231	6.4.5.2. هدف CM ، ALC_CMS
234	6.4.5.3. تحویل ALC_DEL
235	6.4.5.4. امنیت توسعه ALC_DVS
236	6.4.5.5. تصحیح نقص ALC_FLR
238	6.4.5.6. تعریف چرخه حیات
240	6.4.5.7. ابزار و فنون
241	6.4.6. کلاس آزمون‌ها : ATE
242	6.4.6.1. پوشش، ATE_COV
244	6.4.6.2. عمق ATE_DPT
245	6.4.6.3. آزمون‌های کارکردی ATE_FUN
246	6.4.6.4. آزمون مستقل ATE_IND
249	6.4.7. گروه ارزیابی آسیب‌پذیری : AVA
250	6.4.8. گروه ترکیب : ACO
250	6.4.8.1. مولفه‌های کلاس ترکیب



251	6.5 نتیجه گیری
251	6.6 سئوالات آخر فصل
252	6.7 منابعی برای مطالعات بیشتر
254	7. مهندسی امنیت چرخه حیات توسعه
254	7.1 خلاصه فصل
254	7.2 مقدمه
255	7.3 استاندارد ISO/IEC 12207
255	7.3.1 معرفی
256	7.3.1.1 اهداف اصلی آخرین نسخه از ISO/IEC 12207
256	7.3.1.2 چگونگی استفاده
257	7.3.1.3 ضوابط فرایندها
258	7.3.2 فرایندهای توافق (اکتساب)
258	7.3.2.1 اکتساب مقدماتی
260	7.3.2.2 فرایندهای تامین
262	7.3.3 فرایندهای توانمندسازی سازمانی در پروژه
262	7.3.4 فرایندهای پروژه
263	7.3.5 فرایندهای فنی و تکنیکال
265	7.3.6 فرایندهای اختصاصی نرم افزار
265	7.3.6.1 پیاده سازی نرم افزار
266	7.3.6.2 فرایند تحلیل نیازمندی های نرم افزار
266	7.3.6.3 فرایند طراحی معماری نرم افزار
267	7.3.6.4 فرایندهای طراحی تفصیلی نرم افزار
267	7.3.6.5 فرایند ساخت نرم افزار
268	7.3.6.6 فرایند جامعیت نرم افزار
268	7.3.6.7 فرایند تست کیفیت نرم افزار
269	7.3.7 فرایندهای پشتیبانی
269	7.3.8 فرایندهای قابلیت استفاده مجدد نرم افزار
270	7.4 ملاحظات امنیتی در چرخه حیات توسعه سیستم
270	7.4.1 مزایای ادغام امنیت در SDLC
271	7.4.2 مخاطبان این روش
272	7.4.3 دروازه ها و نقاط کنترلی
272	7.4.4 فعالیت های مشترک در همه فازهای چرخه حیات

273.....	7.4.5. پست‌های کلیدی و مسئولیت‌های اصلی در SDLC.....
275.....	7.4.6. فاز آغازین از چرخه حیات.....
275.....	7.4.6.1. مهمترین فعالیت‌هایی فاز آغازین.....
276.....	7.4.6.2. دروازه‌های کنترلی مورد ممیزی در انتهای فاز.....
276.....	7.4.6.3. دسته‌بندی مهمترین بخشهای فاز آغازین.....
279.....	7.4.7. فاز اکتساب /توسعه.....
279.....	7.4.7.1. مهمترین فعالیت‌هایی فاز اکتساب/توسعه.....
280.....	7.4.7.2. دروازه‌های کنترلی مورد ممیزی در انتهای این مرحله.....
281.....	7.4.7.3. دسته‌بندی مهمترین فعالیت‌های فاز اکتساب/توسعه.....
285.....	7.4.8. فاز پیاده‌سازی و ارزیابی.....
285.....	7.4.8.1. مهمترین فعالیت‌های فاز پیاده‌سازی و ارزیابی.....
286.....	7.4.8.3. دسته‌بندی فعالیت‌های این فاز.....
287.....	7.4.9. عملیاتی کردن و نگه داری سیستم.....
287.....	7.4.9.1. فعالیت‌های مهم فاز عملیاتی و نگه داری کردن سیستم.....
288.....	7.4.9.2. دروازه‌های کنترلی مورد ممیزی و بازرسی در این فاز.....
288.....	7.4.9.3. دسته‌بندی فعالیت‌های این بخش.....
290.....	7.4.10. منسوخ شدن.....
290.....	7.4.10.1. مهمترین فعالیت‌های این فاز.....
291.....	7.4.10.2. دروازه‌های کنترلی مورد ممیزی و بازرسی در این فاز.....
292.....	7.4.10.3. دسته‌بندی فعالیت‌های این فاز.....
293.....	7.5. نتیجه‌گیری.....
294.....	7.6. سئوالات آخر فصل.....
294.....	7.7. منابعی برای مطالعات بیشتر.....
296	8. مهندسی امنیت چرخه حیات نرم افزار
296.....	8.1. خلاصه فصل.....
296.....	8.2. مقدمه.....
297.....	8.3. الزامات اساسی مهندسی امنیت.....
298.....	8.4. معرفی SSE-CMM.....
299.....	8.4.1. انواع دسته‌بندی‌های و پیاده‌سازی‌های مختلف.....
299.....	8.4.2. معماری SSE-CMM.....
301.....	8.4.2.1. خصوصیات فعالیت‌های پایه.....
301.....	8.4.2.2. خصوصیات حوزه‌های فرایندی.....



302	8.4.2.3. فعالیتهای عمومی
303	8.4.3. سطوح بلوغ
304	8.4.3.1. بررسی تفصیلی سطوح بلوغ قابلیت
305	8.4.3.2. فرآیندهای موجود در هر سطح بلوغ
306	8.4.4. شفافیت فرآیندها از دید مدیریت در سطوح مختلف بلوغ
307	8.5. مدل‌های ترکیبی مهندسی امنیت
307	8.5.1.1. نگاشت CC به درون SSE-CMM
308	8.5.1.2. تغییر SSE-CMM
309	8.5.1.3. تشریح مدل CC-SSE-CMM
309	8.5.1.4. نگاشت BPها و GPها با توجه به سطوح CC
309	8.5.1.5. فرایند ارزیابی محصول و CC-SSE-CMM به ازای هر سطح
310	8.5.2. معرفی مدل CC-SSE-CMM-CS
310	8.5.2.1. تشریح مدل CC-SSE-CMM-CS
313	8.6. بررسی مدل‌های مهندسی امنیت موجود
313	8.6.1. انواع چارچوب‌های پیاده‌سازی مهندسی امنیت
314	8.6.2. ISO/IEC 2700x و ISO/IEC 17799
315	8.6.3. Assurance Frameworks و CISSP و تکنیک‌های ممیزی و بازرسی
315	8.6.4. ISO 9001
315	8.6.5. خانواده CMMi
316	8.6.6. SSE-CMM
316	8.6.7. CC-SSE-CMM
317	8.6.8. CC-SSE-CMM-CS
317	8.6.9. ISO/IEC 12207
317	8.6.10. Common Criteria
318	8.6.12. جمع‌بندی از بررسی ویژگی‌های در مدل‌های موجود
319	8.7. مدل‌های احتمالی آینده
319	8.7.1. مزایای ISO/IEC 12207 برای ادغام CC
321	8.7.2. پیشنهاد یک چارچوب
322	8.7.3. قواعد و الزامات چارچوب پیشنهادی
322	8.7.4. پیش نیازهای ضروری برای شرح چارچوب
323	8.7.5. گروه‌بندی فازهای تولید نرم افزار
324	8.7.6. شرح چارچوب

325.....	8.7.6.1 اصطلاحات به کار رفته در لایه‌های سوم.....
325.....	8.7.6.2 چگونگی ممیزی و تعیین استقرار کلاسهای تضمین CC در لایه سوم.....
326.....	8.7.6.3 محتویات مستند وضعیت امنیت یا SSD.....
326.....	8.7.6.4 جداول پیشنهادی خانواده‌ها و عناصر کلاسهای تضمین.....
326.....	8.7.6.5 ارائه پست‌های کلیدی امنیت و ممیزی استقرار کلاسهای تضمین CC.....
327.....	8.8 نتیجه‌گیری
327.....	8.9 سئوالات آخر فصل.....
328.....	8.10 منابعی برای مطالعات بیشتر.....
341.....	جدول کلمات اختصاری



Chapter

1

امنیت فن آوری ❁

اهداف فصل

- آشنایی با ضرورت و اهمیت مطالعه امنیت فن آوری
- بررسی مفاهیم پایه به کار رفته در علم امنیت فن آوری اطلاعات و ارتباطات
- بررسی چگونگی ارتباط مفاهیم پایه و چگونگی استفاده از این مفاهیم
- شناخت معنای صحیح چارچوب و مفاهیم اولیه مدیریت ریسک
- مطالعه متریک‌های امنیتی، چگونگی تعریف، طراحی، استفاده و بیان متریک‌ها
- آشنایی با برخی مدل‌های ارزیابی و تحلیل ریسک
- آشنایی با برخی مدل‌های برگشت سرمایه در حوزه امنیت فن آوری

1. امنیت فن آوری



پروفسور رونالد ریوست Prof Ronald L. Rivest

استاد دانشکده کامپیوتر و الکترونیک دانشگاه MIT

از پیشگامان الگوریتم RSA، رمزنگاری، الگوریتم‌های رمز و محرمانگی داده‌ها

1.1. خلاصه فصل

با گسترش روز افزون تجهیزات فن آوری اطلاعات و ارتباطات در طی سالهای اخیر و وابستگی هرچه بیشتر حیات بشری به این سیستم‌ها، جنبه‌های بسیار زیادی از این تعامل تنگاتنگ و غیر قابل انکار مورد مطالعه و ارزیابی قرار گرفته است.

امنیت سیستم‌های کامپیوتری تنها یکی از زمینه‌های مورد بحث در این علم می‌باشد که شرایط نادر و پیچیده‌ای بر آن حکم فرماست. ایده‌های طلایی مطرح شده در این حوزه به سرعت مورد استقبال قرار گرفته و در صنعت، تجارت، پزشکی و غیره مورد استفاده قرار می‌گیرد، ولی ناگهان و با همان سرعتی که رشد یافته است رو به افول نهاده و چالشهای بسیاری را پیش روی سرمایه گذاران قرار می‌دهد. در این فصل ابتدا به بیان برخی ضرورتها پرداخته و پس از بیان مفاهیم بنیادی حوزه امنیت فن آوری اطلاعات، مدل‌های مدیریت ریسک، متریک‌ها و بازگشت سرمایه معرفی می‌گردد.

1.2. مقدمه

جوامع مدرن بشری عمیقاً و به شکل غیر قابل انکاری وابسته به سیستم‌های نرم افزاری در همه ابعاد زندگی مدرن خود هستند. این آمیختگی در همه وجوه حیاتی زندگی بشر امروز از تعاملات کوچک در سطح اجتماع گرفته تا اجرای امورات کلانی چون انرژی، حمل و نقل، صنایع دفاعی ارتباطات، صنایع تولیدی سبک و سنگین و مسائل مالی به شکل روز افزونی به چشم می‌خورد.

مسلم است که در این میان امنیت و صحت کارکرد این سیستمها بسیار حائز اهمیت و بنیادی است و نبود و یا وجود کاستیهایی در مقوله امنیت و کارکرد صحیح این سیستمها بصورت فاجعه باری می‌تواند دنباله ای زخرابی و خسارت را بوجود بیاورد که نهایتاً زندگی و حیات بشریت را تحت الشعاع قرار خواهد داد.



تا زمانی که این سیستم‌های نرم افزاری (در حقیقت مجموعه تجهیزات فناوری اطلاعات و ارتباطات) آسیب‌پذیری‌ها و حفره‌ها را به همراه خود داشته باشند قطعا طعمه‌ای برای مهاجمان و سوداگران خواهند بود. مهاجمان اثرات بسیار مخربی و زیانباری بر سازمانهایی که دست‌اندرکار تولید این سیستمها هستند و یا سازمانهایی که این سیستم‌های اطلاعاتی را به خدمت گرفته‌اند خواهند گذاشت و البته قصه به همین جا ختم نمی‌شود، به هر حال طرف دیگر این خسارت مشتریان (عموم کاربران در هر شکل) و نهایتا تجارت است که تحت این ضرر و زیان‌ها قرار خواهد گرفت و دیری نمی‌پاید که سایه زوال بر صنعت انفورماتیک افکنده خواهد شد.

1.3. معرفی موسسه پونمن¹

قبل از بیان اهمیت و الزام بررسی و مطالعه مهندسی امنیت و ارائه تعاریف، راه کارهای این صنعت، که پیشگامان عرصه فن آوری اطلاعات در سراسر جهان را مجبور به مطالعه و صرف هزینه‌های بسیار گزاف در حوزه‌های مختلف مهندسی امنیت ساخته است، کوتاهانه به معرفی موسسه پونمن وابسته به دانشگاه میشیگان می‌پردازیم.

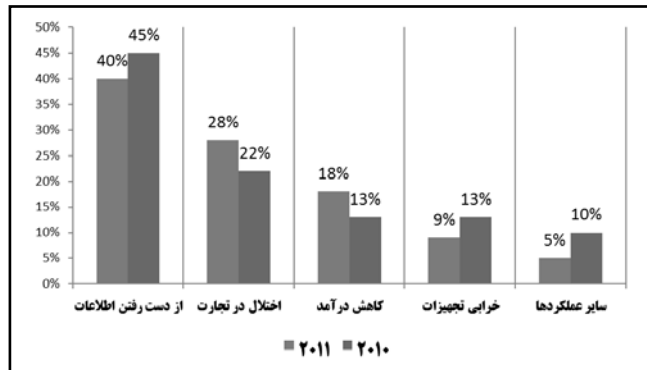
فعالیت محققان این موسسه در مورد بررسی مسائل مختلف در محرمانگی داده‌ها²، حفاظت از داده‌ها³ و تدوین سیاست‌های امنیتی⁴ است و نتایج این تحقیقات ماهانه برای دولت مردان و شرکت‌های بزرگ بعنوان یک معیار سنجش موثق به کار می‌رود. اکنون به تازه‌ترین گزارش این موسسه که در انتهای سال 2011 ارائه شده است توجه کنید[4]:

1.3.1. هزینه‌های ناشی از سرقت اطلاعات

همواره مهمترین بخش از هر تخلف رایانه‌ای خارجی سرقت اطلاعات مهم سازمانها است، در یک گزارش سالانه اطلاعات به سرقت رفته حدود 40 درصد از کل هزینه‌های تخلف رایانه‌ای خارجی این سازمانها را در بر داشته که نسبت به سال قبل 2 درصد کاهش را نشان می‌دهد. ایجاد اختلال در فرایندهای کسب و کار حدود 28٪ که نسبت به سال قبل حدود 6 درصد افزایش را نشان می‌دهد، کاهش درآمد 18 درصد، خرابی تجهیزات و اثراتی که سایر عملکردها داشته اند تا حدی کاهش قابل توجه داشته است.

1. کلیه مطالب این زیر بخش از Ponemon Institute LLC منبع شماره سه شیوه دستیابی به این اطلاعات ذکر شده است.

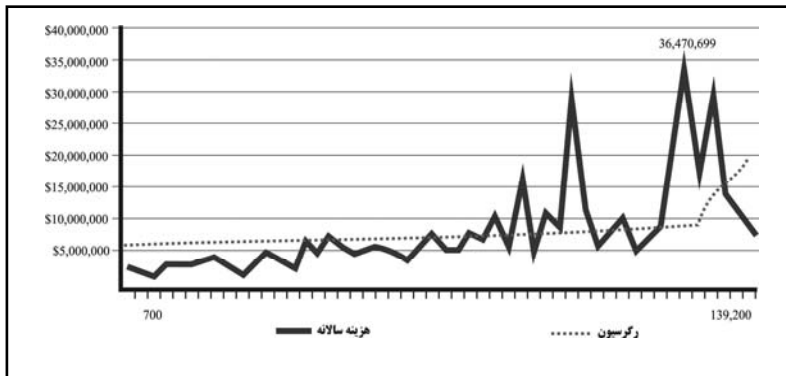
2. Data Privacy
3. Data Protection
4. Security Policy



شکل 1-1 هزینه‌های ناشی از سرقت اطلاعات

1.3.2. توزیع هزینه‌های تخلفات رایانه‌ای بر اساس اندازه سازمان

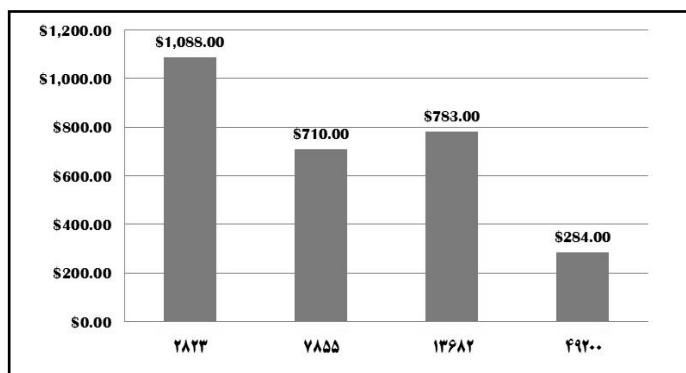
در این گراف اندازه سازمان بر اساس میزان پرسنل سازمانی تعیین شده است، همانطور که در مشاهده گراف می‌کنید، به طور محسوسی با رشد سازمان میزان هزینه جرایم و مشکلات امنیتی هم رشد می‌یابد و این روند طی رگرسیون خطی رشد یابنده (مثبت) نشان داده شده است.



شکل 2-1 توزیع هزینه‌های تخلفات رایانه‌ای بر اساس اندازه سازمان

1.3.3. تحلیل‌های هزینه بر اساس تعداد پست سازمانی

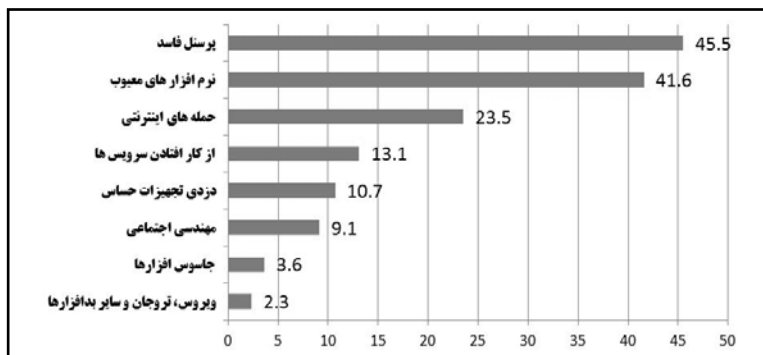
در شکل زیر خلاصه‌ای از تحلیل‌های سالانه هزینه‌های سازمان به نسبت تعداد پست‌های پرسنلی نشان داده شده است، بنابر این نمودار که سازمانها را به چهار دسته تقسیم کرده است، متوسط هزینه سازمان‌های کوچک برای هر پست تقریباً 3.8 برابر متوسط هزینه‌ای است که سازمانهای خیلی بزرگ برای هر پست در مقوله تخلفات و ملاحظات امنیتی تحمل می‌کنند!



شکل 1-3 تحلیل‌های هزینه سازمان بر اساس تعداد پست پرسنلی

1.3.4. متوسط زمان بازیابی سرویس‌ها

در این گزارش که 50 شرکت چند ملیتی در آن شرکت کرده اند، همان‌طور که ملاحظه می‌کنید، میزان متوسط زمان لازم برای موارد پرسنل مختلف و پس از آن نرم افزارهای و حملات به ترتیب بیشترین هزینه‌های مالی و زمانی برای کشف، خنثی سازی و بازیابی سرویس هاپس از ایجاد خسارات را بر سازمان تحمیل می‌کند.



شکل 1-4 تحلیل‌های هزینه سازمان بر اساس تعداد پست پرسنلی

مشاهده می‌شود که با گسترش فناوری، مصدومیت در برابر حملات نیز گسترش یافته است، باید تدابیر امنیتی جدیدی در عرصه فن آوری اطلاعات در نظر گرفت و مهم‌تر از همه اینکه امنیت نرم افزار بعنوان بخش جدا ناپذیر فرایند تولید و توسعه فن آوری اطلاعات است و همه و همه به این معنا است که نیازمند مهندسی امنیت نرم افزار هستیم.

1.4. مفاهیم پایه

در این بخش مفاهیم اصلی که در کلیه مباحث این کتاب به وفور تکرار می‌شوند، مطابق تعاریف ذکر شده در استانداردهای امنیتی بیان می‌شود.

1.4.1. ریسک

ریسک‌های کسب و کار هر سازمان بطور مستقیم بر یک یا چند مشتری هدف آن سازمان اثر می‌گذارد، تشخیص ریسک می‌تواند به شفاف‌سازی و اینکه رویدادهای پیرامون سازمان به چه میزان بر کسب و کار سازمان اثر دارند، کمک کند. ریسک‌های تجاری می‌توانند شامل خسارت‌های مالی، بی اعتباری مارک^۱، تجاوز به حقوق مشتریان^۲، نقض مواضع قانونی، افشاء اسرار مالی و قرار دادی، افزایش هزینه‌های توسعه محصولات و نگهداری سیستم‌های اطلاعاتی جاری و غیره شود. مسئله مهم دیگر شیوه بیان شدت ریسک است که از طریق لغت‌های جاری در دنیای مالی و حسابرسی و متریک‌های مدیریت پروژه همانند ارزش سهام، سود مستقیم، سطح تولید، و هزینه تولید مجدد و غیره بیان شود. مدیران، خصوصاً مدیرانی که پاسخ گوی سرمایه گذاری‌های کلان هستند از مدیریت ریسک بعنوان چارچوبی برای اتخاذ تصمیم‌های مناسب جهت تشخیص، تسهیل، طبقه‌بندی و اولویت‌بندی ریسک استفاده می‌کنند همانگونه که در سالهای اخیر مدیریت ریسک، موفقیت‌های زیادی را خصوصاً در سرمایه گذاری‌های حوزه امنیت فناوری اطلاعات داشته است.

❖ تعریف

تعاریف بسیار زیادی در مورد ریسک وجود دارد. در ذیل چند تعریف استاندارد و جهانی را ارائه می‌دهیم.

الف) تعریف NIST:

ریسک تابع احتمال این است که یک منبع تهدید داده شده از پتانسیل آسیب‌پذیری خاصی استفاده کند و نتیجه اثرات آن به شکل حوادث مضر در سازمان اتفاق بیفتد [3].

ب) تعریف NASA

این سازمان ترکیب احتمال (بطور کیفی یا کمی) اینکه یک برنامه یا پروژه حوادث ناخواسته‌ای را تجربه کند و نتیجه، اثر، یا شدت حادثه ناخواسته در جایی که اتفاق افتاده است را ریسک می‌نامد [8].

1. Brand

2. نقض مشتری مداری

