ملاحضات امنیتی
در سامانه های اطلاعات سلامت

دکتر افشین نیاکان

شرکت دانش بنیان، اطلاع رسانی پیوند داده ها

تعاریف پایه امنیتی در سامانه های اطلاعات

امنیت:

حفاظت در برابر انواع مخاطرات با منشاء انسانی (عمدی / هدفمند)

ایمنی:

حفاظت در برابر انواع مخاطرات با منشاء طبیعی (غیرعمد / غیرهدفمند)

امنیت نرم افزار:

حفاظت در برابر مخاطراتی نظیر: سرقت اطلاعات، دستکاری اطلاعات، رد سرویس و...

ایمنی نرم افزار:

حفاظت در برابر مخاطراتی نظیر: قطع ناگهانی برق، خرابی هارددیسک، اختلال شبکه و...

نتایج عدم رعایت امنیت در سامانه های اطلاعات (سلامت)

چنانچه یک رخداد (نقص) امنیتی از ناحیه یک سیستم نرم افزاری حادث شود، تبعاتی را به دنبال خواهد داشت که این تبعات میتواند چهار گروه مدعی داشته باشد:

1) **امنیت ملی** : ضربه اجتماعی، دفاعی، حقوقی، قضایی و...
2) **شخص حقوقی:** ضربه به کسب و کار، حیثیت، اعتبار، آبرو، رقابت پذیری و...
3) **شخص حقیقی:** ضربه به سلامت جسمی، روحی و روانی، اقتصادی، وجهه اجتماعی و...
4) **شخص ثالث:** ضربه غیر مستقیم از ناحیه دیگری

مزایای افزایش ضریب امنیت نرم افزار از دید مصرف کننده

1) پوشش الزامات کارفرمایی و قوانین فرادستی جهت پاسخدهی به نهادهای فراسازمانی
2) اعتماد به عملکرد سیستم (عدم ایجاد گلوگاه)
3) اطمینان به حفظ اطلاعات و تداوم کسب و کار موجود
4) سهولت در ردیابی سایر چالشهای امنیتی در سازمان مصرف کننده (شبکه، سخت افزار، کاربران و...)
5) معیاری برای تشخیص و انتخاب بهینه محصول مورد انتظار

قوانین و یا استانداردهای مطرح امنیتی در سامانه های اطلاعات

HIPAA :

قانون مسئولیت و قابل انتقال بیمه سلامت
(The Health Insurance Portability and Accountability Act)

ISO 15408:

استاندارد تخصصی ارزیابی سطح امنیتی محصول (نرم افزار، سخت افزار، کارت الکترونیک و....) بر اساس مدل ارزیابی Common Criteria

گروه استانداردهای ISO/IEC 27000 (ISMS):

مدیریت امنیت سیستم های اطلاعاتی Information Security Management System

OWASP:

Open Web Application Security Project

چارچوب CC برای پیاده سازی ISO 15408

- TOE (Target Of Evaluation): همان محصول مورد ارزیابی است که شامل مجموعه‌ای از نرم‌افزارها، سخت‌افزارها و میان‌افزارهای عملیاتی میگردد که هدف مشخصی را دنبال می‌کنند.
- ST (Security Target): سندی حاوی نیازمندی‌های امنیتی برای یک TOE خاص است و کاملاً وابسته به نحوه پیاده‌سازی محصول می‌باشد. این مستند توسط تولیدکننده سیستم تهیه میگردد و در آن به توانمندیها و قابلیتهای امنیتی سیستم خود به دقت و به وضوح اشاره میکند.
- PP (Protection Profile): سندی حاوی نیازمندی‌های امنیتی برای گروهی از TOE ها است که مستقل از پیاده‌سازی آنها می‌باشد. این مستند توسط مشتری (نهاد حاکمیتی) تهیه میگردد و در آن الزامات امنیتی مورد نظر (مورد تقاضا /مورد انتظار) خود را به وضوح مطرح میکند.
- EAL (Evaluation Assurance Level): سطح امنیتی محصول (نرم افزار) بین EAL۱ الی EAL ۷

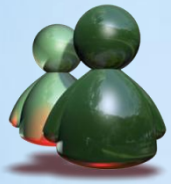
مدل ارزیابی CC برای پیاده سازی ISO 15408

مرکز گواهی ملی
(افتا + وزارت بهداشت)

PP

CC

ST



تولیدکننده

TOE

آزمایشگاه مرجع CC

سطوح تضمین امنیت محصول بر مبنای CC

کلاس تضمین (ارزیابی)

کلاس ارزیابی توسعه (ADV):

کلاس ارزیابی راهنما (AGD):

کلاس ارزیابی چرخه حیات (ALC):

کلاس ارزیابی سند هدف امنیتی (ASE):

کلاس ارزیابی تست (ATE):

کلاس ارزیابی آسیب پذیری (AVA):

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP				**1**	1	**2**	2
	ADV_INT					**2**	**3**	3
	ADV_SPM						**1**	1
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**
Guidance documents	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
Life-cycle support	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD			**1**	1	1	1	**2**
	ALC_TAT				**1**	**2**	**3**	3
Security Target evaluation	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**3**	3	**4**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5

چرا ملاحضات امنیتی در سامانه های اطلاعات سلامت اهمیت بیشتری دارد؟

- در صورت سرقت شماره کارت بانکی، شما می تونید کارت بانکی و یا حتی بانک خود را عوض کنید.
- اما در اکثریت کشورها از جمله آمریکا نمیتونید کارت سلامت خودتان را کنسل کنید یا شناسه یکتای سلامت خود را عوض نمایید.
- تغییر در اطلاعات سلامت می تواند جان فرد را به خطر بیندازد.
- پس سرقت اطلاعات هویتی بخصوص سلامت اهمیت زیادی دارد.
- با این وجود تنها بین سالهای ۲۰۰۵ الی ۲۰۰۸ ۴۰ میلیون رکورد اطلاعات پزشکی به علت رخنه اطلاعاتی تنها در آمریکا به سرقت رفته

قانون حفظ حریم خصوصی Privacy Rule

- ✓ قانون حفظ حریم خصوصی در ۱۴ آپریل ۲۰۰۳ در آمریکا اجرایی شد.
- ✓ حریم خصوصی اشاره به حفاظت از اطلاعات فردی مراقبت های بهداشتی دارد
- ✓ مشخص می کند که اطلاعات بیماران چگونه استفاده و افشا گردد.
- ✓ به بیماران اختیار می دهد که کنترل بیشتری بر اطلاعات سلامت خود داشته باشند.
- ✓ راه های صیانت از اطلاعات سلامت را مشخص می نماید

.

- ➢ قوانین HIPAA برای ایجاد تعادل منطقی بین جریان آزاد اطلاعات و صیانت از حریم خصوصی بیماران وضع گردیده

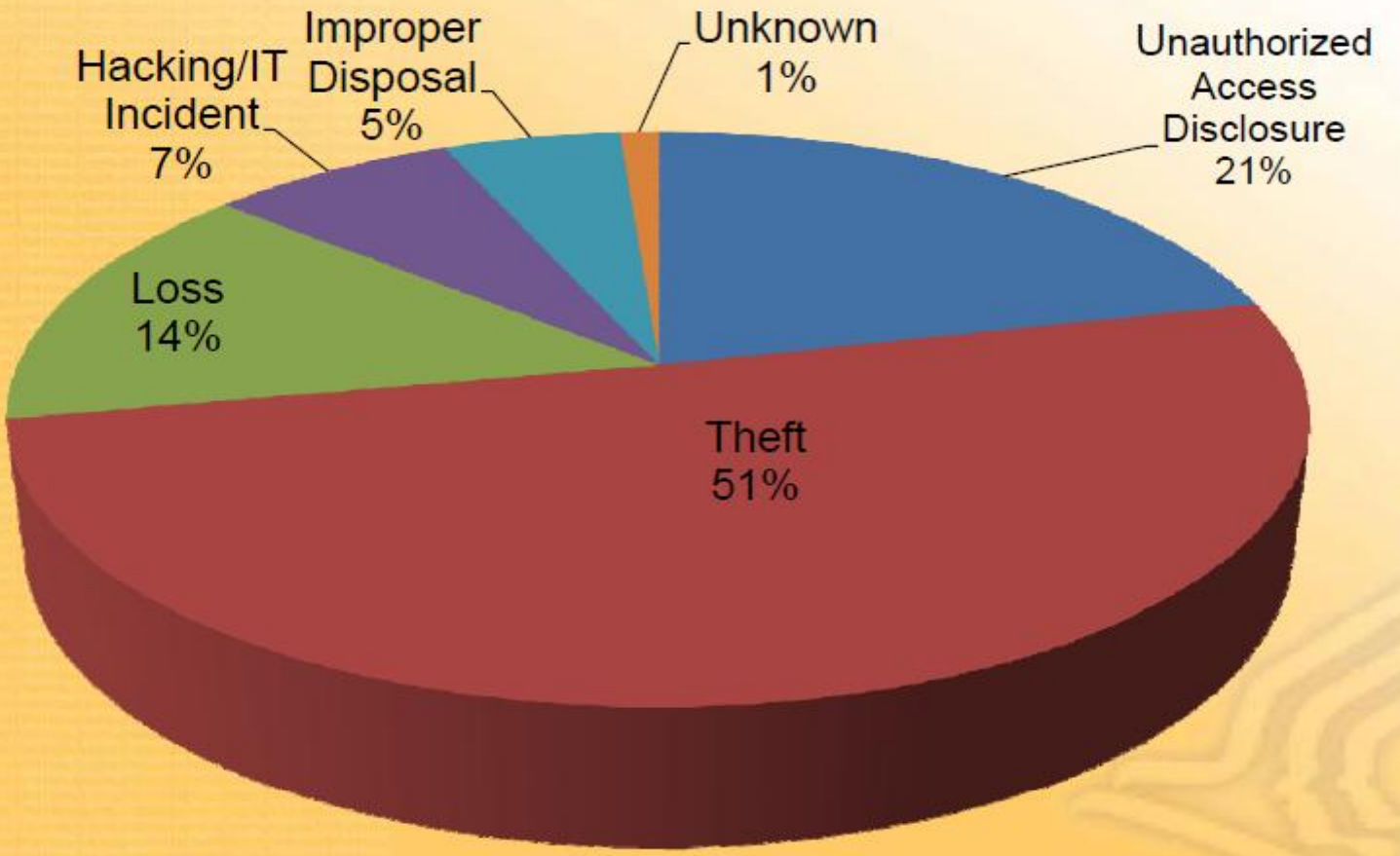
مشکلات امنیتی
در
دنیای واقعی سلامت الکترونیک

مطابق با گزارشات واحد خدمات بهداشتی، انسانی

دفتر حقوق مدنی OCR (ناظر HIPAA)

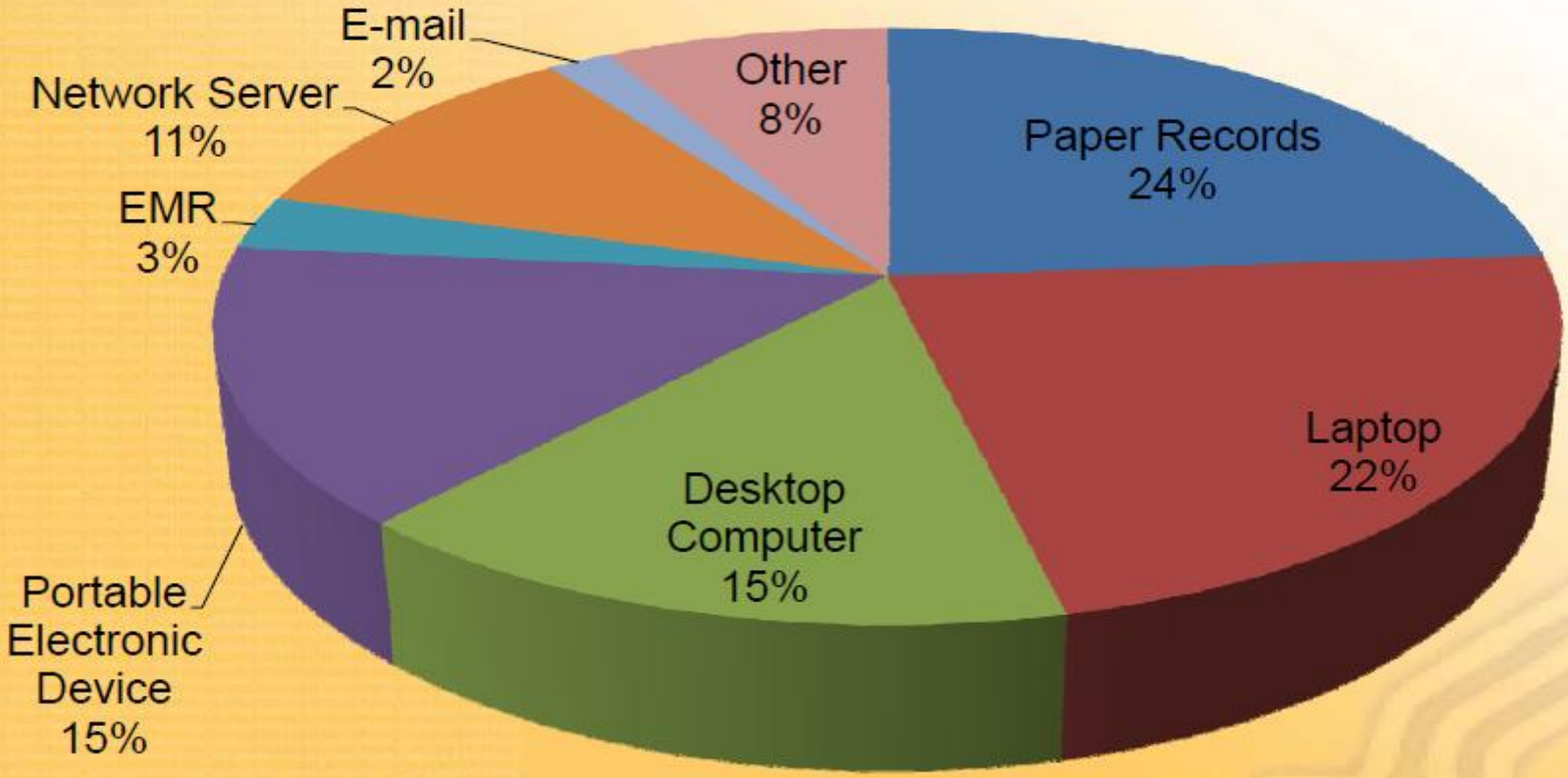
Office of Civil Right

Breach Notification:
500+ Breaches by Type of Breach



OCR

Breach Notification:
500+ Breaches by Location of Breach



OCR

امنیت HIPAA موارد زیر را پوشش می دهد

- حفاظت اداری
- حفاظت فیزیکی
- حفاضت فنی (امنیت سیستم و امنیت برنامه ها و داده‌ها)

با تشکر:

دکتر افشین نیاکان

اطلاع رسانی پیوند داده ها