How to Increase Project Success with Risk Analysis
정보 위험 분석을 통한 프로젝트 성공법

00:00 – 01:24
안녕하세요. 엘라 블룸입니다. 8 월 웨비나를 시청해주셔서 감사합니다. 이 시간은 여러분들의 마이크와 헤드셋을 조정하는 시간입니다. 조금 전 들으셨던 음악은 강연자의 목소리보다 더 크게 나오니 강연 중에는 볼륨을 조금 크게 설정하시기 바랍니다.

자 그럼 본격적으로 시작해보겠습니다. 먼저 시청해주셔서 감사합니다. 그렉 바셋 PMP 가 이번 웨비나에서 강연을 하게 된 것을 저희는 매우 기쁘게 생각합니다. 그는 클리어워터 컴플라이언스에서 서비스 제공 부사장으로 활동하고 있는 정보 보안 분야의 전문가입니다. 또한 연방 의료정보보호법(HIPPA)과 생명 과학, 제조, 임상, 실험실 품질 관행, 결제 카드 산업의 데이터 기준, IT 소프트웨어 개발 주기 등 다양한 분야의 법규 준수에 있어 많은 경험을 보유하고 있습니다.

그럼 이제 그렉 바셋씨의 강연을 시작해보도록 하겠습니다. 시작해주십시오.

01.25 –
대단히 감사합니다. 이렇게 좋은 자리에서 강연할 수 있는 기회를 주셔서 감사합니다. 저는 여러 해 동안 프로젝트 관리사로 활동해왔습니다. 저는 이런 웨비나들이 양질의 정보를 제공한다는 사실에 늘 감탄해왔습니다. 제 강연이 그러한 기대를 충족시킬 수 있기를 희망합니다.

오늘 저는 정보 위험 분석과 그 중요성에 대해서 설명 드리고자 합니다. 강연을 시작하기 전에 법적인 부분에 대하여 한 가지 당부의 말씀을 드리겠습니다. 강연 내용에는 법률 자문이 포함되지 않습니다. HIPPA-HITEC/PCI 와 같은 규제에 관한 설명이 포함되어 있지만 이는 법률 자문으로 간주되어서는 안됩니다. 여러분들이 진행하는 프로젝트에 대해서는 반드시 법률 전문가의 자문을 구하시기를 바랍니다. 그럼 먼저 저에 관하여 짧게 소개할까 합니다. 저는 네트워크와 엔지니어에서 소프트웨어 개발, 지난 몇 년간은 정보 보안 분야에 이르기까지 IT 분야에서 오랫동안 활동해왔습니다.

클리어워터 컴플라이언스에 대하여 간략하게 소개해 드리자면 저희는 수백 만 미국인들의 개인적인 건강관련 정보를 관리하는 기관들이 안전하게 정보를 관리할 수 있도록 도와주는 역할을 하고 있습니다. 주로 HIPPA 첨단 기술 준법 분야를 위주로 하며 고객들이 소송에 연루되지 않도록 돕고 있습니다. 우리는 일부 의료 기관의 웹사이트들이 데이터 손실이나 규정 위반을 범한 경우를 쉽게 접하게 됩니다. 의료산업 종사자라면 피하고 싶은 곳이죠.

그럼 먼저 위험 분석과 관리가 왜 필요한 지에 관하여 설명 드리겠습니다. 가장 근본적인 7 번은 IT 와 비즈니스 전략 실행에 있어 꼭 필요한 것입니다. IT 와 비즈니스 전략을 실행하려면 다방면에서 잘 짜인 위험 관리 프로그램이 필요합니다. 지속적인 프로세스 개선의 근간이 되기도 합니다. 어떤 위험이 존재하는지 이해하고 비즈니스가 요구하는 사항을 파악하는 것은 지속적은 프로세스 개선을

위해 매우 중요합니다. 이를 통해 정보 체계에 대한 많은 지식을 얻을 수 있기 때문에 교육적인 측면에서도 값진 경험이 됩니다. 사용 방식에 대한 의도와 실제 사용 방식에 대하여 이해할 수 있게 됩니다. 또한 프로세스상에서 나타나는 흥미로운 차이점도 확인할 수 있습니다. 이러한 차이점을 극복할 수 있는 해결 방안을 수립하는데도 도움이 됩니다. 위험 분석은 기초 보안 프로그램을 구축하는데 있어 반드시 필요한 과정입니다.

많은 규제와 요건들은 일종의 위험 관리를 위한 수단이 되기도 합니다. HIPAA 는 위험 분석에 관하여 직접적으로 규정하기도 합니다. PCI DSS 또한 하향식 위험 분석을 규정합니다. 이는 보안 사고를 예방하는데 도움이 되는 일종의 도구라고 할 수 있습니다. 언론을 통해서 이미 들으셨을 테니 기관들에 얼마나 심대한 타격을 주는지에 대해서는 따로 말씀 드리지 않겠습니다. 하지만 꼭 피해야 하는 것들입니다.

그렇다면 어떤 위험이 있고 위험의 정도는 얼마나 될까요? 오래된 타이어를 예로 들어보겠습니다. 타이어로 그네를 만들었다고 가정해보겠습니다. 여기서 위험 요소와 자산, 위협에 대한 취약성은 어떻게 파악할 수 있을까요? 여기서 자산은 타이어로 만든 그네입니다. 즉 즐거움을 위한 놀이기구입니다. 위협과 취약성은 낡은 밧줄이 될 수 있습니다. 잠재적인 위험은 밧줄이 끊어져 발생할 수 있는 부상을 들 수 있습니다. 즉 자산과 위협을 파악하고 위협에 대한 보호장치를 마련하는 것입니다.

그럼 위험 분석의 다음 단계에 대하여 살펴보겠습니다. 이것들은 일반적으로 고려해야 하는 항목들입니다. 위험 분석을 진행하는데 있어 많은 잘못된 방식들이 있습니다. 처음 프로세스를 진행하면 많은 업무가 요구됩니다. 지름길은 없습니다. 하지만 시간이 지나면 수월해집니다. 한 번 하고 잊어버릴 수 있는 것들이 아닙니다. 현실에서 가장 중요한 감사 및 조사 결과입니다. 의료 및 인적 서비스 분야에서 시민의 권리보호를 위해 가장 중요한 부분입니다. 여기에 대한 슬라이드가 있습니다. 위험 분석은 위험 처리가 아닙니다. 위험 분석은 서버에 패치를 적용하는 것을 의미하지 않습니다. 완전히 다른 서비스입니다. 지속적인 프로세스 개선이 요구되는 작업입니다.

그렇다면 어떻게 위험을 분석하고 관리할 수 있을까요? 이때 고려해야 할 사항은 무엇일까요? 이것은 민권 웹사이트에서 가져온 자료입니다. 먼저 이 차트를 살펴보면 중앙에 빨간 선이 있습니다. 이것은 교정활동에 대한 계획입니다. 세로축은 교정활동에 대한 계획이고 상단에 가로축은 다양한 기업들에 걸쳐 실시된 여러 시행 활동들입니다. 수치들은 각종 요건을 위반하여 부과된 벌금을 의미합니다. 이들 기업들의 공통점은 조사를 실시하거나 위반사항이 발견되기 전까지 위험 분석을 실시하지 않았다는 점입니다. 50~59 개의 제공자들의 경우 최소 하나의 보안 위반사항이 발견되었습니다. 이들 기업들의 3 분의 2 가 위험 평가나 분석을 실시하지 않았습니다. 보안 관련 시행사항에 대한 위반이 없는 기업들은 모든 관련사항들을 시행한 것으로 나타났습니다. 따라서 위험 분석을 실시하면 민권과 관련된 문제가 발생하지 않는 것을 알 수 있습니다. 감사 주안점에 대하여 살펴보겠습니다. 초년도에 감사를 실시한 기업들입니다. 위험 분석을 실시하고 있습니까? 어떤 방식으로 위험을 관리합니다. 다음 연도는 사업 동업자에 대한 관한 것입니다. 이러한 쟁점들은 사업 동업자들에 대한 위험 분석과 관리에도 확장될 것입니다. 이에 따라 의료 분야와 같은 세부 산업에도 중요하게 됩니다. 위험 분석은 준법에 있어서 핵심적인 부분입니다.

이러한 문제에 관하여 앞으로 설명을 드릴까 합니다. 우리가 해결해야 하는 문제는 무엇일까요? 여기에는 개인정보, 신용카드 정보, 지적 재산 등 보안이 필요한 모든 정보가 포함됩니다. 우리가 보호하고 싶은 정보들이죠. 만일 내 비밀정보가 공유된다면 어떻게 해야 할까요? 내 정보가 누구와 공유되며 어떤 방식으로 공유되는지 알아야 합니다. 이것은 보안에 관한 문제입니다. 반면 내 정보가 완전하거나 정확하지 않거나 최신화되어 있지 않다면 어떻게 해야 할까요? 의료분야를 예로 들자면 병원에서 내 혈액형을 잘못 알고 있는 경우입니다. 이것은 매우 심각한 문제입니다. 무결성에 대한 문제이죠. 꼭 필요한 정보가 없는 경우도 마찬가지 입니다. 이것은 가용성에 대한 문제입니다. 따라서 우리가 해결해야 하는 문제는 정보의 기밀성과 무결성, 가용성을 보장하는 것입니다. 이 세 가지 중 어느 하나도 간과해서는 안됩니다. 따라서 정보 보안과 위험 분석은 기밀성과 무결성, 가용성을 모두 보장하는 것을 목표로 합니다.

10:15 – 20:20
이 단계에서 우리가 취해야 하는 행동은 무엇일까요? 먼저 법규에서 정한 요건을 정확하게 숙지하는 것입니다. 예를 들어 HIPAA 에서는 위험 분석을 요구하고 있습니다. PCI DSS 또한 위험 분석을 요구합니다. 저는 전력 발전이나 전자 제품 분야에 적용되는 규정들을 조사하고 있습니다. 이들 분야에서도 위험 분석을 요구하고 있습니다. 규정을 준수하려면 위험 분석을 실시해야 합니다. 하지만 이들 규정의 취지가 무엇인지 파악하고 위험 분석을 제대로 수행하기 위한 관련 지침을 이해하는 것이 중요합니다.

위험과 위험 분석에 대한 용어도 알아야 합니다. 강연 후 관련 용어가 나와있는 블로그 링크를 공유해 드리겠습니다. 클리어워터에서는 과학 기술 연구소에서 정한 기준들과 문서, 지침들을 중요하게 생각합니다. 학습하는데 매우 유용한 자료들이죠.

또한 위험 분석에 해당하지 않는 것들에 대해서도 명확히 알고 있어야 합니다. 패치 적용이나 제어는 해당되지 않습니다. 위험 분석은 위험을 파악하는 프로세스입니다. 위협요소와 취약한 부분은 무엇이고 이들이 정보 자산과 어떻게 연관되는지, 이러한 위협이 발생할 가능성이 얼마나 되는지 파악하는 것입니다. 여기에 대해서는 나중에 자세하게 설명 드리겠습니다.

이제 방법을 정해야 합니다. 여러 방법들이 있습니다. 매우 복잡한 과정을 거쳐야 하기 때문에 방법을 스스로 고안하는 것은 어렵습니다. 이미 다수의 효과적인 방법들이 존재하기 때문에 이들 중에 적합한 것을 선택하기만 하면 됩니다.

이제 위험 분석을 실시합니다. 위험 분석을 실시하고 위험관리 계획을 수립한 후 최소 1 년에 한 번 위험 분석을 수정하는 작업을 합니다. HIPAA/HITECH 규정에서는 주기적으로 위험 분석을 업데이트할 것을 요구하고 있습니다. 저희는 연단위로 실시할 것을 권장합니다. 하지만 기업의 특성에 따라 지속적인 개선 활동을 실시하는 것이 필요합니다. 사업 계획에 포함시키고 IT 전략이나 관련 프로젝트의 모든 단계에 반영해야 합니다.

위험이 무엇인지 완벽하게 이해하고 있는 사람은 얼마 되지 않습니다. 따라서 위험이 무엇인지 먼저 설명하겠습니다. 여기 그래픽 자료를 보겠습니다. 우리 모두는 자산과 가치를 가지고 있습니다.

그것은 개인 정보가 될 수도 있고 다른 가치를 지닌 정보를 의미하기도 합니다. 정보의 소유자는 위험을 최소화하고자 합니다. 위협요소는 악의적, 우발적, 구조적, 환경적인 요소들로 구분됩니다. 위협요소는 자산을 악용하고 손해를 초래합니다. 이러한 위협요소가 발생하면 위험은 증가하게 됩니다.

보안 체계가 가진 취약성을 악용하는 위협요소들도 존재하며 이는 위험을 가중시킵니다. 소유자는 이러한 취약성을 인지하고 위험을 감소시킬 수 있는 통제 및 보안 수단을 마련해야 합니다. 이러한 통제나 보안 수단이 취약성의 원인이 되어 위험을 초래하기도 합니다. 위험 분석의 핵심은 위험이 미치는 영향을 파악하는 것입니다. 즉 정보의 기밀성과 무결성, 가용성을 얼마나 저하시키는지를 의미합니다. 우리는 자산, 위협요소, 취약성, 통제수단, 발생가능성을 단순히 공식에 대입하여 위험성을 파악할 수 있기를 바랍니다. 이러한 단순 공식을 활용하는데 있어서 문제점은 각각의 항목과 변수, 자산, 위협요소, 취약성, 통제수단이 변한다는 점입니다. 발생가능성 또한 비즈니스 환경에 따라 변합니다. 모든 요인들이 변하기 때문에 지속적인 비즈니스 프로세스를 통해 반영하는 것이 필요합니다. 과거에 사용되어온 방법들을 살펴보겠습니다. 클리어 워터에서는 NIST 에서 발행한 800-30 교정본 1 의 위험 평가 지침을 참고하고 있습니다. 이에 관해서는 다음 슬라이드에서 설명 드리겠습니다. 저희는 이 지침을 HIPAA HITEC 준수를 위한 위험 분석 소프트웨어와 서비스 플랫폼에 적용하고 있습니다. 저는 최근 수행한 C 등급 위험 인증서를 어제 전달받았는데요. 이것은 IT 코드 5 를 학습하는데 매우 중요한 부분을 차지합니다. 이 중에는 이메일 프레임워크도 있고 ISO 에서 정한 ISO 27002 도 있습니다. 또한 요소 분석을 위한 정보 위험 지침도 있습니다. 이들은 모두 위험 분석 시 활용할 수 있는 유용한 방법들입니다. 위험 평가를 준비하는데 쉽게 적용할 수 있는 프로세스를 가지고 있습니다. 그럼 위험 분석을 실시하는 과정을 설명 드리겠습니다. 가장 먼저 할 일은 위험 평가를 준비하는 것입니다. 위협에 대한 원인과 취약점, 선행조건, 발생 가능성, 영향을 파악합니다. 지속적으로 위험 평가를 실시하는 것이 중요합니다. 관련 이해관계자들과 정보를 공유합니다. 결코 복잡하지 않습니다. 물론 세부적인 사항들은 짚고 넘어가야 합니다.

저희는 8 단계로 구성된 위험 분석 프로세스를 권장합니다. 단계별로 살펴보면 먼저 데이터를 수집합니다. 위험 분석의 폭은 기업의 전체 규모와 정보 체계에 따라 결정됩니다. 범위를 정하고 따르는 것이 필요합니다. PMP 교육에서 파악한 범위를 참고하는 것도 유용합니다. 위험 분석에서는 범위가 많은 문제를 초래할 수 있습니다. 범위를 확장하는 것은 매우 쉽지만 위험 분석은 문서로 작성해야 하고 어떤 범위에서 분석을 실시할지 염두해 두어야 합니다. 데이터 수집 시 고려해야 할 것은 정보 자산 인벤토리에 관한 것입니다. 중요 정보가 어디에 속하는지 파악해야 합니다. 여기에는 많은 예시가 있습니다. 의료분야와 HIPAA/HITEC 로 돌아가 보겠습니다.

18:13 – 18:19 (침묵)

18:20 – 20:19
저희 소프트웨어에서 캡쳐한 화면입니다. 스프레드시트나 워드에 이 정보 자산 인벤토리를 확인할 수 있습니다. 민감한 데이터가 어디에 저장되는지가 중요합니다. 기록에 따르면 보험료 지불 시스템이라는 것을 알 수 있습니다. 약 7 천 개의 기록들이 프로세스 디렉터리를 가리킵니다. 즉 정보 소유자입니다. 하지만 그 이상으로 정보 자산의 상세 내역이 존재합니다. 얼마나 많은 데이터가

어디에 있고 누가 소유하고 있을까요? 이 경우 보험료 지불 시스템은 노트북 등 다른 종류의 미디어를 통해 접속되고 있습니다. 수익과 현금흐름과 같은 중요 정보도 포함되어 있습니다. 각 정보들의 중요성도 제 각각이기 때문에 차이점을 문서로 기록하는 것이 중요합니다.

자산을 파악한 후 다음으로 고려해야 할 사항은 접근 매체의 유형입니다. 잠재적인 위협 요소와 취약점을 파악하기 위한 것입니다. 어떤 위협적인 행위와 원인이 존재하고 취약점은 무엇이며 어디에 정보가 있는지 파악하는 것이죠. 스프레드 시트로 작성하여 모든 것을 관리할 수 있습니다. 노트북을 예로 들어 보겠습니다. 여기에는 다수의 위협 요소와 위협 요소의 유형, 위협 행위, 취약점이 존재합니다. 따라서 핵심 정보를 파악해야 합니다. 노트북은 도난이나 분실 등 다양한 위험 상황이 발생할 수 있습니다. 위협 행위는 분실된 장치에 저장된 정보에 접근하는 행위입니다. 여기에 취약점이 존재하는 것이지요. 도난 당한 노트북의 비밀번호를 풀면 손쉽게 저장된 정보에 접근할 수 있습니다. 강연 중에 노트북에 대한 예시를 몇 가지 더 들어보겠습니다.

20:21 – 30:09
위협 행위와 원인, 취약점을 파악하는 곳은 여러 곳이 있습니다. 미국 국토안보부의 데이터베이스를 통해 이러한 정보를 얻을 수 있고 저희 소프트웨어를 이용하여 분석을 실시할 수 있습니다. 이러한 도구를 활용하여 위협이 발생하는 원인과 행위, 취약점을 확인할 수 있습니다. 보안 인력을 동원하여 국가 보안 데이터베이스를 지속적으로 감시하고 최근 현황을 파악하는 것이 효과적입니다. 여기서 고려해야 할 사항이 많습니다. 이러한 일을 처음 진행한다면 상당한 시간과 노력이 필요합니다. 이렇게 잠재적인 위협 요소와 취약점을 파악하면 이제 현재 실시하고 있는 보안 조치를 확인해야 합니다. 정보 보호를 위해 지금 어떤 보안 조치를 실시하고 있는가? 여러 가지 통제 조치를 취하고 있을 것입니다. 각각의 자산과 위험 요소, 취약점은 상호작용을 통해 위험 수위를 가중시킵니다. 자산은 악용할 수 있는 취약점과 위협요소를 가지고 있으며 이에 대한 통제와 보안 수단이 필요하게 됩니다. 통제 수단에는 여러 가지 유형이 있습니다. 예방적인 통제 수단이 있는가 하면 위협을 방지하거나 감지, 교정, 보완하는 통제 수단도 있습니다. 하지만 위험 분석은 이러한 통제 수단을 파악하는데 그치지 않습니다. 준법 전문가와 지속적으로 협의하여 규정에서 정한 특정 통제 수단에 대한 요건을 충족시켜야 합니다. 예를 들어 PCI 를 준수하기 위해서는 신용카드 정보 데이터를 암호화하는 것이 필요합니다.

따라서 이 슬라이드는 이러한 점을 제대로 반영하지 않고 있죠...

위협 요소와 영향, 취약점은 주황색으로 표시되어 있습니다. 위협 원인은 위협 행위를 초래하여 취약점을 악용하고 피해가 발생합니다. 방지적 성격의 통제 수단은 위협 행위의 발생 가능성을 감소시켜줍니다. 방지적 통제 수단은 네트워크 상에 구축된 예방 및 감지 시스템을 의미합니다. 네트워크의 정상적인 동작을 기준으로 위협 행위를 감지합니다. 감지적 성격의 통제 수단은 위협 행위나 가능성을 발견하여 예방적 통제 수단을 가동시킵니다. 이렇게 위협 행위를 감지하면 네트워크 운용 센터에 통보하게 됩니다. 예방적 통제 수단은 취약점을 보호하고 피해를 최소화해 줍니다. 보완적 통제 수단은 취약점을 악용하는 위협 행위의 가능성을 줄여줍니다. 이렇게 다양한 종류의 통제 수단이 마련되어 있습니다. 교정 통제는 정보 자산에 미치는 영향을 줄여줍니다. 예를 들어

정보를 백업하는 것은 예방적 차원의 통제 수단이며 복구 작업은 교정 수단이 됩니다. 마지막 단계에 가서 데이터를 복구하여 영향을 줄이는 것이지요.

이러한 통제 수단을 통해 취약점이 가진 문제를 해결할 수 있습니다. 또 하나 예를 들어 보면 비밀 정보가 저장된 노트북의 경우 위협 행위는 도난이 됩니다. 여기서 취약점은 노트북이 휴대용이고 비밀번호가 취약하거나 데이터가 암호화나 백업이 되어 있지 않다는 점이 될 수 있습니다. 통제 수단은 보안 정책과 절차, 교육을 마련하고 비밀번호, 인증장치, 암호화, 원격 데이터 삭제, 백업과 같은 보안 조치를 강화하는 것입니다.

이와 관련하여 여러 가지 통제 지침이 마련되어 있습니다. FISMA (연방정보보안관리법)에서는 일련의 통제 규정을 정하고 있습니다. NIST 통제지침에서도 800-53 통제 예규와 등급을 정하고 있습니다. ISO 27002 도 통제 예규를 정하고 있습니다. 이들을 조합하여 정보 체계를 구축할 수 있습니다. 그렇다면 실시하고 있는 보안 통제는 어떻게 평가할 수 있을까요? 스프레드 시트를 작성할 수 있습니다. 저희 소프트웨어 화면을 하나 보여드리겠습니다. 상세한 분석과 교차 분석이 가능합니다. 로그인 실패가 반복되면 계정이 잠기는 정책을 실시하고 가정하면 기본적으로 이에 대한 매트릭스를 구축해야 합니다. 특정 통제 자산에는 적용되지 않을 수도 있습니다. 결국 이런 식으로 보여지게 됩니다. 노트북을 통해 접근하는 정보 자산이나 보험료 지불 시스템이 있다면 저희 소프트웨어에서는 노트북의 위협요소와 취약점을 조합한 체계가 마련되어 있습니다. 그리고 NIST 800-53 에서 정한 통제 요건을 충족할 수 있습니다. 위협 요소와 행위, 취약점의 측면에서 보면 노트북이 도난 당하거나 분실되면 누구든 노트북에 저장된 정보에 접근할 수 있게 됩니다. 이러한 취약점과 사용자 인증수단에 초점을 맞추고 적합한 윤리적 통제 수단을 강구해야 합니다. 이것은 두 가지 요소를 결합한 인증체계 입니다. 사용자가 로컬로 인증하는 것이지요. 만일 두 가지 요소를 결합한 인증체계가 존재하지 않고 로컬로만 인증한다면 위험 분석은 이렇게 보여집니다. 각각의 미디어 유형에 대하여 이러한 위험 분석을 실시하게 됩니다.

그 다음에는 발생 가능성과 영향을 결정해야 합니다. 일반적으로 이 두 요소는 동일한 단계에서 진행되기 때문에 이 둘을 조합하기도 합니다. 위협 요소가 발생할 가능성과 발생 시 미치는 영향을 파악하는 것입니다. 즉 발생 확률이 얼마나 되고 그 영향은 무엇인지 정하는 것입니다. 저희는 발생 가능성을 1~5 나 1~10 의 점수로 산정합니다. 5 단계의 점수 체계를 활용합니다. 얼마나 자주 발생하는지를 고려하여 순위를 정하게 됩니다. 결코 발생하지 않는 경우에서 확실히 발생하는 수준의 범위에서 정해지게 됩니다. 그렇다면 위협 상황이 발생할 확률은 무엇일까요?

영향도 마찬가지입니다. 부정적인 상황 발생에 대한 정의와 점수표, 피해 또는 손실에 대한 지침이 마련되어 있습니다. 위험의 영향도도 가장 치명적인 수준에서 미미한 수준인 0~5 까지의 수치로 정해집니다.

가능성과 영향에 대한 체계가 마련되었으면 이제 점수를 평가합니다. 이것도 스프레드 시트를 작성합니다. 암호화가 되어 있지 않은 노트북을 도난 당한 경우를 예로 들어 보겠습니다. 이런 일이 발생할 확률은 얼마나 될까요? 이 경우 영향도는 5 점입니다. 이렇게 모든 점수가 매겨지면 모든 자산에 대해서도 점수를 매깁니다. 5-5, 1-3, 3-5 와 같이 위험 수준을 평가합니다.

위험 분석가의 관점에서 생각하는 것이 중요합니다. 이 슬라이드가 아마 큰 도움이 될 것입니다. 보안 위험은 자산을 보호하기 위해 마련된 통제 수단의 취약점을 악용하는 경우 발생합니다. 이는 피해와 비용을 초래합니다. 그것이 전부입니다. 어떻게 보면 단순하죠. 위험 분석은 계획 중이거나 실행 중인 보안 통제를 고려하여 위험을 파악하고 우선순위를 설정하고 산정하는 일련의 과정입니다. 이것을 보면 쉽게 이해할 수 있습니다. 5 단계의 프로세스를 통해 정보 보안 책임자나 IT 책임자에게 어떤 위험이 존재하며 자산을 보호하기 위해 마련된 통제 수단의 어떤 취약점이 악용될 수 있는지 설명할 수 있습니다. 이것은 위험이 존재하는 경우에 해당되죠.

가능성과 잠재적인 영향력이 모두 확인되면 이제 현재 위험 수준을 파악할 수 있습니다. 4, 5 단계가 완료되면 6 단계는 매우 쉽습니다. 발생 확률을 영향도에 곱하기만 하면 됩니다. 이렇게 5 단계 영향도 점수와 5 단계 발생 확률 점수를 산정했으니 이제 표를 만들어서 점수를 합산합니다. 영향도와 확률을 곱하면 (5 x 5) 25 점이 됩니다. 이런 방식으로 위험 수준과 비용을 산정할 수 있습니다.

30:10 – 41:14
이제 다시 스프레드 시트를 활용합니다. 발생 확률인 5 와 영향도인 5 를 곱해 25 점의 위험 평가 점수가 매겨졌습니다. 다른 모든 자산과 위협 요소, 취약점에 대해서도 점수를 매겨야 합니다. 이런 작업을 위한 도구가 있으면 매우 유용하죠. 자동화된 스프레드 시트가 있으면 편리합니다. 특히 규모가 큰 조직이나 프로그램에 더욱 그러합니다. 이 때 딜레마가 발생합니다. 규모가 클수록 더 많은 사항들을 고려해야 하죠. 모든 자산과 미디어 유형, 위협 요소, 원인, 취약점, 가용한 통제 수단을 고려해야 하기 때문입니다. 저희가 소프트웨어를 개발하면서 내부적으로 평가한 결과 약 3 억 3 천 만개의 순열이 발견되었습니다. 너무나 방대한 양이죠. 이 모든 것을 검색할 수는 없습니다. 보시는 것처럼 분석 범위가 넓을수록 순열의 수도 증가합니다.

따라서 저희 소프트웨어는 다음과 같은 방식으로 위험 수치를 산정합니다. 보험료 지불 시스템에 대한 정보가 저장된 노트북이 있다고 가정해보겠습니다. 이 경우 위협 요소로 노트북을 관리하는 IT 담당자의 부주의를 들 수 있습니다. 통제 수단으로는 미디어 재사용에 관한 정책이나 보안 정책, 인력의 보안 교육을 들 수 있습니다. 이 중에는 진행단계에 있는 것도 있고 이미 실행되고 있는 것도 있습니다. 따라서 위험 등급을 정합니다. 조직에 부정적인 영향이 발생할 가능성과 취약점이 악용될 수 있는 가능성을 파악하는 것이죠. 그리고 부정적인 영향의 심각성을 평가합니다. 이 경우 발생 가능성은 2 이고 위험 등급은 10 점이 됩니다.

그 다음 할 일은 문서작업을 완료하는 것입니다. 규제 수준과 환경을 이해하는데 있어 매우 중요합니다. 왜냐하면 지금 실행하고 있는 통제 수단이 규제 요건을 충족해야 하기 때문이죠. 이를 위해서는 자산 내역 보고서가 필요합니다. 먼저 민감한 데이터가 어디에 있는지 파악해야 합니다. 이것만으로도 쉽지 않은 작업입니다. 고객의 신용카드 정보가 어디에서 처리되고 저장되는지 알고 있습니까? 어떤 경우에는 예, 어떤 경우에는 아니오라고 대답하게 되죠. 의료 분야에서는 자신의 전자 건강 기록이 어디에 저장되어 있는지 파악하는 일입니다. 업무 과정을 고려해서 그러한 기록들이 어디로 전달되는지 확인해야 합니다. USB 에 저장되어 있을까요? 아니면 엑셀 파일로 저장되어 있을까요? 아니면 누군가의 이메일에 저장되어 있을까요? 아니면 주말에도 일을 할 수 있도록

누군가의 개인 이메일에 저장되어 있을까요? 개인의 건강기록뿐만 아니라 지적 재산, 금융정보, 신용카드 정보도 보호해야 합니다. 이러한 내역은 매우 중요하고 수집하기도 어렵습니다. 지속적으로 관리를 해야 하는 부분입니다. 민감한 데이터가 많을수록 이들이 여기저기 돌아다닐 확률은 더 커집니다. 따라서 이러한 내역이 항상 최신상태로 유지되도록 지속적인 관리가 필요합니다. 또한 자산 내역을 올바로 기록하는 일에도 노력을 기울여야 합니다.

다음에는 위험 분석 방법을 보여줍니다. 즉 업무 내용을 보여주는 것이지요. 해당 정보 자산과 데이터에 접근하는 미디어에 대한 위협 요소와 취약점을 파악한 것을 보여줍니다. 각 자산에 대한 발생 확률과 영향도를 산정하여 위험 등급을 평가한 것을 보여줍니다. 이렇게 진행한 업무 내용을 보여줍니다. 그 다음은 분석 범위입니다. 모든 민감한 데이터는 위험 분석에 포함되고 문서화되어야 합니다. 해당 문서와, 잠재적인 위협 요소, 취약점을 파악하고 현재 가용한 보안 조치를 확인합니다. 즉 이러한 데이터를 보호하기 위해 실행하고 있는 조치를 의미하죠. 위협요소와 발생 가능성을 파악하고 발생 시 미치는 영향을 파악합니다. 이를 통해 위험 등급을 평가합니다. 그리고 이를 문서화하여 주기적으로 업데이트합니다. 규모가 큰 조직의 경우 1 년에 한 번 포괄적인 위험 분석을 실시할 것을 권장하고 있습니다. 체계가 보다 잘 확립된 조직의 경우에는 이러한 위험 분석을 그들의 프로젝트와 비즈니스 계획 수립 전략, IT 전략에 반영하기도 합니다. 그들은 위험 분석 결과를 활용하기를 원합니다. 그들은 민감한 정보가 어디에 있고 어떤 위협요소와 취약점, 위험이 존재하는지 알고 있습니다. 프로세스 시스템을 교체하는 경우 관리 기록을 열람하여 해당 위험 점수가 20 점이 되는지 먼저 확인합니다. 신규 시스템으로 위험 수준이 감소할 수 있는지, 보안 장치로 위험 점수가 줄어드는지, 또 이에 대한 대응 조치가 마련되어 있는지 검토합니다. 이렇게 위험 분석을 실시한 후에는 위험 관리의 다음 단계를 진행할 수 있게 됩니다.

이제 위험 등급이 어떤 시스템으로 어떻게 분포되는지 알아야 합니다. 방사선학 시스템을 갖춘 저희 소프트웨어를 예로 들면 46 개의 낮음, 27 개의 중간, 4 개의 높음, 2 개의 치명적 등급으로 분류됩니다. 이것으로 위험에 대한 분포를 설명할 수 있습니다. 이는 경영진에서 활용할 수 있는 매우 유용한 정보로 감사나 규제 전문가의 검토를 요구하기도 합니다.

이것은 위험 등급에 대한 다른 관점입니다. 자산별 위험 등급이죠. 가장 위험한 자산은 무엇인가? 어떤 자산이 가장 높은 위험성을 가지고 있고 어떤 조치를 취할 것인지 알아야 합니다. 이것은 특히 IT 전략 수립에 유용하죠. 위험성 감소를 위해 IT 시스템에 투자를 한다면 어디에 투자를 할 지 파악하는데도 도움이 됩니다. 위험 분석 없이는 추측에 의존할 수 밖에 없습니다. 포괄적이고 개선된 위험 분석을 통해 어디에 투자를 해야 하는지 정확하게 파악할 수 있습니다. 예를 들어 시스템상의 위험성에 따라 환자들의 데이터 보안에 투자를 하는 것이지요. 이것은 등급 검토와 파악된 위험성을 보여주는 분석 보고서입니다. 모든 미디어 장치와 자산, 위협 활동, 점수가 목록으로 작성되어 있습니다.

이러한 위험을 관리하는데 있어 핵심은 위험에 대한 허용치가 파악되면 모든 위험을 감소시키는데 총력을 기울일 필요는 없다는 점입니다. 위험은 어디에든 존재합니다. 비즈니스를 하는 것 자체가 위험을 감수하는 것이죠. 아침에 노트북을 키는 것도 위험하죠. 노트북에 화면이 켜지지 않고 그 자리에서 사망할 수도 있습니다. 기업도 어느 정도의 위험은 감수해야 합니다. 위험에 대한 허용치는

기업마다 다르지만 어떤 허용치가 어떻게 정해지는지 이해하는 것이 중요합니다. 저희 소프트웨어의 화면입니다. 이 기업의 위험 허용치는 9 입니다. 따라서 9 보다 낮은 위험성은 감수하는 것입니다. 10 이상의 위험은 대응 계획을 수립하고 실행에 옮깁니다. 이렇게 위험에 대한 허용치가 마련되어 있음을 보여주어야 합니다. 모두가 이를 알고 있어야 합니다. 모든 위험성을 일일이 설명할 필요는 없습니다.

위험성을 해결할 때에는 이런 방식으로 대안을 평가할 수 있습니다. 존재하는 위험을 파악하고 이에 합당한 판단을 내려 대책을 수립하는 것입니다. 다시 노트북을 예로 들어보겠습니다. 2 단계 인증과 사용자의 로컬인증이 있습니다. 모두 매우 효과적인 방법입니다. 비용을 산정하고 타당성 조사를 실시하여 대책을 세운 것이지요. 특정 대안을 도입하거나 거부할 수 있습니다. 이런 방식으로 업무과정을 보여주거나 검토할 수 있으며 IT 전략과 프로젝트 수행 시 반영할 수 있습니다. 이를 통해 위험관리 계획을 수립할 수 있습니다. 우측에는 대안에 대한 평가와 책임자 등 위험 처리에 대한 방식이 나와있습니다. 각 위험성에 대한 책임자가 있음을 보여주는 것이 중요합니다. 그들은 위험성이 허용치를 넘으면 조치를 취하게 됩니다.

마지막으로 주기적으로 검토와 업데이트를 실시합니다. 한 번으로 끝나는 작업이 아닙니다. 지속적인 관리가 필요합니다. 보안 문제가 발생한 조직을 살펴보면 3~4 년 전에 마지막으로 검토 작업을 수행한 것을 흔하게 볼 수 있습니다. 하지만 IT 종사자들에게 3~4 년 전은 암흑기나 마찬가지입니다. IT 는 끊임없이 변화합니다. 사업 환경도 마찬가지죠. 위협요소와 취약점도 뉴스를 통해 아시는 것처럼 끊임없이 변화합니다. 따라서 이러한 주기적인 검토작업이 필요합니다. 저희는 1 년에 한 번 할 것을 권장하고 있으며 프로젝트와 기업에 따라서 더 자주 실시해야 합니다. 시스템을 개선이 이루어질 때마다 간략하게 위험 분석을 실시하는 것이 좋습니다. 교체 작업이나 아웃소싱을 하는 경우에도 해당 시점에 위험 분석 평가를 실시해야 합니다.

41:15 -
진행 중인 비즈니스 프로세스가 있다면 지속적인 노력이 필요합니다. 그에 걸맞은 위험 분석을 실시해야 합니다. 동일한 방법을 지속적으로 활용하여 개선이 이루어지고 있음을 보여줘야 합니다.

결론적으로 위험 분석을 제대로 실시하면 대중의 신뢰를 얻을 수 있고 노출된 위험성을 파악하고 합당한 의사결정을 내릴 수 있습니다. 이는 모든 비즈니스와 IT 환경에 핵심이 됩니다. IT 와 비즈니스 전략에서 중요한 것은 지속적인 프로세스 개선이며 이를 통해 상당한 교육 효과를 얻을 수 있습니다. 이러한 과정을 통해 팀은 시야를 넓히고 IT 조직에 대한 관심을 가지게 됩니다. 개선 계획을 수립하여 IT 전략과 프로젝트 계획에 반영하는데 도움이 되기도 합니다. 보안 프로그램을 수립하는데 있어 기본적인 과정으로 꼭 필요한 작업입니다. 많은 규정들이 이러한 위험 분석을 요구하고 있으며 일상 업무에서 보안 사고와 위반을 예방하는데 도움이 됩니다. 누구도 CHS 와 같이 보안 사고의 희생자가 되거나 이해관계자와 이사회에 보안사고에 대한 공지를 띄우고 싶지 않을 것입니다. 위험 분석 없이는 효과적인 예방이 불가능합니다.

마지막으로 여기 참고가 될만한 자료들이 있습니다. 슬라이드의 링크를 웨비나 블로그에 올려드리겠습니다. 이것으로 강연을 마치겠습니다. 이제 질문에 답하는 시간을 갖도록 하겠습니다.

43:25 – END
진행자: 멋진 강연 감사합니다. 제가 질문을 읽어 드리겠습니다. 질문 내용을 확인하시는 동안 채팅창에서 질문을 받고 있겠습니다. 질문이 있으신 분은 해주시기 바랍니다.

1. 법규를 위반한 회사 목록은 어느 웹사이트에 나와 있나요?

미국 보건복지부의 민권사무소입니다. HIPPA 법집행을 담당하는 지부로 "Law of Shame"이라고 불립니다. 웹사이트에 방문하거나 구글에서 "OCR wall of shame"이라고 검색하면 아마 첫 번째 링크에 표시될 것입니다.

2. 네트워크 설정 하자로 인한 영향에 관한 질문입니다. 이로 인한 광범위한 취약성을 위험 분석에서 어떤 방식으로 다뤄야 하나요?

네트워크 설정 하자는 여러 측면에서 설명이 가능합니다. 어떤 방식으로 영향을 평가할 것인가? 기밀성과 가용성, 무결성 측면에서 살펴봐야 합니다. 이 세 가지 요소를 보호해야 합니다. CIA 정보 보안을 생각해보십시오. 네트워크 설정 하자는 데이터 유출을 초래하여 기밀성을 저하시키고 사용자의 보안 위반이나 네트워크 접근을 허용합니다. 설정 오류가 무엇인지에 따라 무결성, 즉 네트워크가 불안정해지고 잠재적인 영향을 초래합니다. 가장 드문 경우는 가용성이죠. 설정 오류로 인하여 네트워크가 불안정해지면 신뢰성에 문제가 생기로 데이터에 접근할 수 없게 됩니다. 예를 들어 운용실에서 전자 모니터링 시스템을 사용하고 있고 업데이트를 위해 네트워크에 연결되어 있는 경우 네트워크가 불안정하다면 잠재적인 영향은 그만큼 커지게 됩니다. 여러 방법으로 어떤 영향을 미치는지 파악해야 합니다. 다수의 영향을 미칠 수 있으며 위험 분석을 통해 최악의 상황을 고려해야 합니다. 이를 통해 어떤 네트워크 설정 항목인지 파악합니다. 그것이 네트워크 스위치인지 서버인지 노트북 또는 데스크탑의 네트워크 설정인지 알아내야 합니다. 그리고 이에 따른 잠재적인 영향은 무엇인지 파악해야 합니다. 가용한 통제 수단을 적용한 후 이에 따른 영향을 측정하는 것이 중요합니다. 이미 실행 중인 통제 수단을 평가합니다. 예를 들어 노트북의 경우 네트워크 설정이 중앙에서 관리되면 사용자가 네트워크 설정을 변경할 수 없습니다. 그러면 문제의 발생 확률이 감소되고 이에 따른 영향도 감소하게 됩니다. 좋은 질문이었습니다.

진행자: 답변 감사합니다.

3. 경험에 비춰볼 때 자산 평가 시 가장 세부적인 평가 대상으로 무엇을 권장하시나요?

자산은 정보를 의미합니다. 가장 세부적인 평가 대상은 임계성에 기반합니다. 병원의 경우에는 노트북입니다. 즉 노트북이나 노트북의 메모리까지 포함시키지 않죠. 하지만 전자 그리드 시스템이나 제조시스템의 경우에는 개별 구성요소를 확인합니다. 더 세부적으로 확인하기도 합니다. 다시 말씀드리지만 보호하고자 하는 정보의 기밀성과 무결성, 가용성에 어떤 영향을 주는지 고려해야 합니다. 그리고 어느 시점에 구성요소가 관여하는지 알아야 합니다. 저장 네트워크나 서버, 하드 디스크를

분석 대상으로 합니다. 분리된 장치의 경우 취약성과 그로 인한 위협요소를 고려합니다. 일반적으로 위협에 대한 취약성을 기준으로 범위를 설정합니다.

4. 인적 요소와 관련된 위험성을 줄이는 방법으로 무엇을 권하고 가장 심각한 알려지지 않은 위험에는 어떤 것이 있나요?

물론 인력을 줄여 이에 따른 위험을 감소시킬 수 있습니다. 인간은 실수를 범합니다. 수많은 절차와 통제 수단이 있으며 교육이나 인식을 고취시키기도 합니다. 민권사무소의 위반 사례를 살펴보면 차 뒷좌석에 놓아둔 노트북이나 미디어가 도난 당하거나 분실되어 발생한 경우를 확인할 수 있습니다. IT 전문가들에게는 왜 차 뒷좌석에 노트북을 놓아두는지 이해하기 어렵지만 사람이기 때문에 그러한 실수를 하게 됩니다. 따라서 지속적인 보안 교육이 필요합니다. 매년 정보 보안 교육을 실시하여 위협요소와 취약성에 대한 인식을 고취시켜야 합니다. 보안 위반에 대한 뉴스가 나면 인식 교육을 실시하기에 적합합니다. 인적 요소에 대한 위험은 이러한 교육으로 대응합니다. 사람들의 인식을 고취시키고 교육과 올바른 도구를 제공하는 것입니다.

5. 위험 분석은 평균적으로 얼마나 걸리나요?

정말 좋은 질문입니다. 강연 초반에 말씀 드린 것처럼 그것은 설정 범위에 따라 달라집니다. IT 프로젝트에 대한 위험 분석을 실시하고 이전에 실시한 적이 있다면 몇 주 정도가 소요될 것입니다. 하지만 대기업의 경우 더 많은 사람들이 관여하게 됩니다. 의료기관의 위험 분석 워크숍을 진행하는 경우 약 6~8 주가 소요됩니다. 이를 위해서는 기관에서 많은 시간을 투자하고 최소 2 명의 분석가가 워크숍 진행을 위해 고용되어야 합니다. 일반적으로 6~8 주가 소요되고 이는 중간에서 대규모 조직에 해당되죠. 소규모 의료기관의 경우 하루나 이틀이 소요되기도 합니다. 실무자와 몇 시간의 면담을 진행하고 약 4 시간에 걸쳐 자산을 파악하여 위험 분석 계획을 수립합니다. 그리고 결과 보고서를 제공하죠. 결국 소요 시간은 조직의 규모에 따라 결정됩니다.

6. 위험 회피와 완화 중 더 나은 전략은 무엇인가요?

위험 회피는 더 이상 실시하지 않고 있는 방법입니다. 신용카드 결제가 위험하니 현금만 받겠다는 말과 같죠. 이것이 위험 회피 전략입니다. 위험 완화 전략은 신용카드 결제가 위험하지만 모든 신용카드 정보 처리를 아웃소싱해서 시스템상에 정보가 저장되지 않도록 하는 것입니다. 이런 방식으로 위험 완화 활동이 이루어집니다. 물론 그것이 어떤 위험인지, 기업의 위험에 대한 임계치가 얼마인지에 따라 대답은 다릅니다. 어느 정도까지 위험을 감수할 수 있는지가 중요하죠. 좋은 질문이었습니다.

7. 웹 애플리케이션 분석에는 어떤 방법론이 적합할까요?

저희가 권하는 방법론은 기술적으로 NIST 에 적용 가능한 것들입니다. 어떤 기술에도 적용이 가능하죠. 웹 애플리케이션과 표준 IT 인프라 서버를 보유한 기업, 워크스테이션에도 적용이 가능합니다. 이러한 프레임워크는 IT 전체 범위에 걸쳐 적용이 가능합니다. 모든 효과적인 위험

분석에 적용 가능한 취약성 분석을 위한 특정 도구나 의문 사항이 있을 수도 있습니다. 그것이 상위 10 가지의 취약성에 대응하는 공개 웹 애플리케이션 보안 프로그램에 적용가능한지는 확인이 필요합니다. 제가 개인적으로 권하는 방법입니다. 하지만 기존의 대다수 위험 분석 프레임워크는 웹 애플리케이션에 적용이 가능합니다.

8. 강연 초반에 발급 받은 인증서에 대하여 언급하셨는데 어떤 것인지 궁금합니다.

네 최근에 정보 시스템 통제 기관에서 C-Risk 인증을 받았습니다. 정보 보안 및 위험에 관한 인증이지요. 그 기관에서 발급하는 여러 인증들 중에 하나로 위험 관리와 통제에 초점을 맞추고 있습니다. 제가 받은 것은 위험 및 정보 시스템 통제에 관한 것으로 IT 종사자와 희망자들에게 IT 위험 관리 및 기업 위험 관리 인증을 제공하는 제도입니다. 저희 서비스 제공팀 전원이 이 인증을 받았습니다. 방대한 양의 지식을 필요로 하고 시험을 본다는 점에서 PMP 와 비슷합니다. 시험은 미국에서 6 월과 12 월에 실시합니다. 저희는 6 월에 시험을 치렀고 시험에 합격하려면 다양한 위험 및 정보 통제 분야에 대한 경험을 입증해야 하고 제 3 자를 통해 경험 수준을 테스트합니다. 그것이 제가 받은 인증입니다.

진행자: 답변 감사 드리고 축하 드립니다. 오늘 이렇게 위험 분석과 보안에 대하여 강연해주셔서 감사 드립니다. 많은 분들이 좋은 의견과 질문을 주신 걸로 봐서 값진 시간이 된 것 같습니다. 오늘 받은 질문들은 블로그를 통해서도 확인이 가능하니 많은 참여 부탁 드립니다. 다시 한 번 알차고 수준 높은 강연을 해주신 그렉에게 감사를 드립니다. 다음에도 기회가 되면 강연을 해주시기를 희망합니다.

그렉: 강연을 할 수 있도록 기회를 주셔서 감사합니다.

진행자: 참여해주신 모든 분들께 감사 드리며 이것으로 강연을 마치겠습니다. 안녕히 계십시오.